10.17625/NKE.2022.034

Doktori (PhD) értekezés

Som Zoltán

2021. 07. 29

NEMZETI KÖZSZOLGÁLATI EGYETEM
Közigazgatás-tudományi Doktori Iskola

Som Zoltán

Az információbiztonsági tudatosság kérdései a közigazgatásban

Doktori (PhD) értekezés

Témavezető:

Dr. Szádeczky Tamás

Budapest, 2021

TARTALOMJEGYZÉK

1. BEVEZETÉS

1.1. A TÉMA AKTUALITÁSA ÉS JELENTŐSÉGE

Felgyorsult világunkban a tanulás keretei egyre szélesebbek. A tanulási folyamatban résztvevők igényei, magatartása gyökeresen átalakul. A tudás mennyisége folyamatosan növekszik, egyre komplexebb, összetettebb tudás szükséges az informatikai rendszerek működtetéséhez, használatához. Az egész életen át tartó tanulás (ún. lifelong learning) alapkövetelmény. A lexikális, elméleti tudás helyett a tudásalapú gazdaság és társadalom, a munkakörnyezet túlzott dinamizmusa miatt inkább az egyén adaptív és innovatív készségei fejlesztendők. Az önálló tanulni tudás és akarás képessége teszi lehetővé az állandóan változó környezethez való sikeres alkalmazkodást és a személyes megújulást. A jól teljesítő szervezetek sikerének egyik oka, hogy a vezető- és szervezetfejlesztés a szervezeti stratégia része. Olyan befektetés, amely a szervezet hosszú távú eredményes és hatékony működését biztosítja. A tanulási-oktatási kihívás komplexszé vált (folyamatos időhiány, stressz, multitasking, folyamatos változás stb.), ami hagyományos képzési formák segítségével nem kezelhető. A munkatársaknak jellemzően nagyon kevés ideje van kiszállni a pörgő mókuskerékből. Olyan támogatásra van szükségük, amely a lehetőségekhez képest egyénileg róluk szól, időalap-kímélő, praktikus, mégis folyamatos, önállóan is elvégezhető önfejlesztést tesz lehetővé. Ehhez újszerű oktatási módszerek kombinációja szükséges. Az információbiztonsági kihívások ezzel párhuzamosan pedig megkövetelik, hogy az aktuális, gyorsan változó kockázatokra, támadási vektorra egy emberként tudjon reagálni a munkaszervezet. A 2013. évi L. (az állami és önkormányzati szervek elektronikus információbiztonságáról szóló) törvényt az Országgyűlés a 2013. április 15-i ülésnapján fogadta el, a kihirdetés napja 2013. április 25. Még ebben az évben megkezdődött a Nemzeti Közszolgálati Egyetemen (NKE) az Elektronikus információbiztonsági vezető (EIV) szakirányú továbbképzési szak oktatása, mellyel elindult a magyarországi információbiztonsági vezetők egyetemi képzése, és amely képzésben a kezdetektől részt vettem. Információbiztonsági képzéseket azonban már ezt megelőzően, 2010-től aktívan tartottam az EU Safer Internet Program keretében önkéntes oktatóként. Ezt megelőzően pedig a Szegedi Tudományegyetem munkájában vettem részt oktatóként is.

A nemzeti kibertudatossági szinten és ennek összetevőjeként értékelhető közigazgatási kibertudatossági szinten keresztül az egyéni kibertudatosság szerepe folyamatosan felértékelődik, és amíg információs rendszerekkel kapcsolatban nemzeti és gazdasági ellenérdekek vannak, addig vélhetőleg nem is fog csökkenni. Azaz a megfelelő információbiztonsági szint nemcsak egyéni

vagy munkaszervezeti érdek, hanem nemzeti és nemzetgazdasági szinten is fontos. Egyrészt a magánérdekek mentén, másrészt állami szempontból az ügyfélbizalom, valamint az információs rendszerekbe és elektronikus állami szolgáltatásokba vetett bizalom szempontjából is.

Itt szükséges röviden kitérnem a közigazgatás értelmezésére és a szükséges szűkítések megfogalmazására. A Nemzeti Közszolgálati Egyetem kiadványa (NKE, 2020) így fogalmaz: "A közigazgatás a végrehajtó hatalomnak az a tevékenysége, amelynek eredményeként a társadalom tagjai és szervezetei magatartását ténylegesen befolyásolja, mégpedig az állami közhatalom (impérium) birtokában végzett döntés-előkészítés, döntés, végrehajtás és ellenőrzés során, elkülönült állami szervezet által végzett jogalkalmazás (jogérvényesítés), szervezés és a jogalkotásban való közreműködés által." A meghatározás tevékenységként definiálja a közigazgatást. Felépítését tekintve a közigazgatási feladatok ellátásának rendszere: Államigazgatási szervek, Egyéb közigazgatási feladatot ellátó szervek, Közigazgatási feladatot ellátó nem közigazgatási szervek, és Önkormányzati igazgatási szervek lehetnek. Terjedelmi okokból ennél részletesebb kibontásra nincs lehetőségem, azonban azt szükséges hangsúlyozni, hogy több szempontból (elhelyezkedés, geolokáció, szolgáltatási profil, biztonsági besorolás, egyéb) rendkívül eltérőek, mondhatni, hogy munkakörök tekintetében is erősen diverzifikált a közigazgatás. Így ebből következik, hogy amíg nemterjed ki a mérés (vizsgáztatás) tételesen minden egyes munkavállalóra, addig a mintavételezés eredménye függhet (amennyiben nem reprezentatív) a csoport kiválasztásától és nagyságától. A disszertációmban bemutatott kutatás ennek megfelelően nem a közigazgatás egészére, nem annak minden egyes munkavállalójára kiterjedő mérés, nem reprezentatív mintának tekinthető. Itt természetesen a kiugrások, kiemelkedő eredmények vagy elmaradások nem mutathatóak ki egyedi válaszadókig, hanem egy kérdőív kitöltőire igaz következtetés vonható le. Statisztikailag elveszik benne az egy-egy kiugró eredmény, ugyanakkor a nagy tömegekről, adott időpontra vonatkoztatva egy megközelítőleg jó, pontos képet mutathat.

A közigazgatás mellett említést kell tenni az e-közigazgatásról is, amely évek óta folyamatosan megvalósul, azaz egyre elterjedtebb a használata mind a közigazgatásban, mind pedig a felhasználói oldalon, az állampolgároknál. Budai (2016) így fogalmaz: "Az e-közigazgatás kialakítása olyan kényszer, amelyet az információs társadalom egymást feltételező (társadalmi, technológiai, szociális, politológiai, jogi stb.) összetevői diktálnak." Így érinti tehát mind a közigazgatásban dolgozókat, mind pedig nemzeti, közigazgatási szinten az összes olyan állampolgárt, aki ügyeket kíván intézni; később pedig lehetséges európai uniós folyamatokkal történő összekapcsolása is megjelenhet, vagy gondolhatunk egyéb nemzetközi közigazgatási kapcsolatokra, állami és nemzetközi tevékenységekre. Ez viszont nemcsak szigorúan véve vett

közigazgatási fejlesztéseket kíván, hanem a kompetenciák, tudás fejlesztése is szükséges. Budai (2016) így fogalmaz: "Bármilyen meglepő, a közigazgatás modernizációjának felhasználói oldala a nélkülözhetetlen kompetenciák fejlesztésénél: az írástudás oktatásánál kezdődik, mely egyre inkább a digitális írástudás dimenziói felé mozdul el. A járulékos kompetenciák pedig biztosítják az önálló továbbfejlődés, élethosszig tartó tanulás (life long learning, LLL) lehetőségét. A felhasználókat tehát képezni kell, így az erre irányuló programokat (…) a közigazgatási megújítás ütemtervéhez kell igazítani. Egyúttal erősíteni kell azokat a támogató programokat, melyek a közigazgatási szolgáltatások hatékonyabb állampolgári igénybevételét támogatják: ügysegédlet, IT-mentorálás." Valamint könnyen belátható, hogy el nem választható rész kell, hogy legyen az információbiztonsági kompetenciák fejlesztése is, ahol a felhasználói oldal túlnyúlik a közigazgatásban dolgozókon; a közigazgatási szolgáltatásokat igénybe vevőkre is gondolni szükséges.

2013-as L. törvény, majd az azt követő 41/2015 BM végrehajtási rendelet, illetve az ágazatspecifikus (17/2019. (VIII. 15.) BM utasítása; a Belügyminisztérium és a belügyminiszter által irányított szervek elektronikus információbiztonsággal összefüggő biztonságtudatos viselkedési kódexe kiadásáról) rendelet kapcsán látható, hogy törvényi szinten megjelent az igény, hogy a fejlődés érdekében szervezett információbiztonsági oktatások valósuljanak meg. Ezen folyamatok már 1994-ban megkezdődtek, az Informatikai Tárcaközi Bizottság 8. sz. ajánlásával, címe: Informatikai biztonsági módszertani kézikönyv. Majd ezt követte időben az Informatikai Tárcaközi Bizottság ajánlásai közül 1996-ban a 12. sz. ajánlás, melynek címe: Informatikai rendszerek biztonsági követelményei. 2008-ban pedig a Közigazgatási Informatikai Bizottság 25. számú ajánlása Magyar Informatikai Biztonsági Ajánlások (MIBA) címmel, amely voltaképpen egy ajánlás gyűjtemény. Valamint egyéb ágazatspecifikus, de mégis információbiztonságot érintő fontos jogszabályok a zártsági tanúsítás előírása a 2008. évi XL. tv. 100§ (1b), (törvény a földgázellátásról) valamint a 2011. évi CCIX. tv. 63§ (törvény a víziközmű-szolgáltatásról).

A baseline mérés és kiértékelés utáni oktatások és azok kiértékelése révén meghatározhatóvá válnak az információbiztonsági fejlesztés kritikus területei. Dolgozatomban a továbbiakban az információbiztonsági baseline kifejezés helyett, a jelenállapot kifejezést fogom használni. Voltaképpen a jelenlegi szint mérése (As-Is állapot) azért fontos, hogy azt követően mérhető, nyomon követhető legyen, legyenek a változások. Az elmúlt évek során, 2013 óta oktatási tapasztalataim alapján látható, hogy nem tartunk még ott, hogy a közigazgatási információbiztonsági felelősök szervezett módon eszközt kapjanak, vagy önszerveződő módon egy ilyen folyamat elinduljon. Fontosnak tartom megemlíteni, hogy több kezdeményezés is létezik, hogy ezen információbiztonsági felelősök szakmai kapcsolatokat tudjanak egymással

vagy piaci szereplőkkel építeni, ám ennek célja és funkciója más. Személyes és oktatási tapasztalataim, azonban határosak, az oktatásban résztvettekre korlátozódnak és természetesen munkaszervezetenként eltérőek. Kijelenthető azonban, hogy az információk (a fentebb bemutatott információbiztonsági ajánlások) és törvényi feltételek adottak. Ezért is tűztem ki ennek vizsgálatát, hogy objektív módon lehessen vizsgálni a tényeket, feloldani azt a látszólagos ellentmondást, amit egy-egy munkaszervezetben vett egy-egy kiscsoportos mintából, az oktatás során kapott visszajelzéseket. Az eltérések azonban már ott is jelentkeztek, hogy hogyan tudták ezt a szervezetek alkalmazni, hogyan értelmezték az ajánlásokat és a jogszabályokat, mit értettek oktatás alatt, hogy ment át szabálykövetésbe. Disszertációmban azonban kizárólag az információbiztonsági oktatással kapcsolatos, meghatározott kérdéseket vizsgáltam. Ezen, egyes szervezetekre jellemző tényező nem került vizsgálatra, hogyan értelmezték az ajánlásokat, jogszabályokat, hogyan építették be a folyamataikba.

Mindezek alapján személyes küldetésem és dolgozatom célja, hogy objektív kutatási adatokat vizsgáljak a felmért időintervallumban. Célom, hogy ezek azonosítása révén lendületet vehessen, és kidolgozott megoldási javaslataim révén feloldható legyen az esetlegesen vagy egyes munkaszervezetekben jelentkező fejlesztések és fejlődés gátja. Ezáltal a közigazgatási információbiztonsági szintet követően mint egyik jelentős összetevőn keresztül a nemzeti kibertudatossági szint is számottevő és mérhető növekedésnek indulhasson.

A blokkoló tényezők, a gyökérokok abban rejlenek, hogy a közigazgatásban Információbiztonsági felelős vagy vezető pozíciót betöltő képesített munkavállalók nem kapnak eszközöket a kezükbe a felkészítésük során és azt követően sem arra, hogyan tudnak információbiztonsági oktatást tartani, tágabb értelemben az információbiztonsági tudatossági szinten fejleszteni. Kifejezetten utalva itt a Nemzeti Közszolgálati Egyetem EIV képzésére, valamint a disszertációmban bemutatott egyéb, Magyarországon elérhető felsőfokú vagy nemzetközi minősítést adó információbiztonsági képzésekre is. Disszertációmban azonban kizárólag a Magyarországon elérhető képzések és minősítések bemutatására szorítkoztam és a magyar közigazgatást és magyar üzleti szférát vizsgáltam. Ennek okai a terjedelmi korlátok, a külföldi mintavétel és felmérés idő és költség korlátai, valamint eddigi oktatási tapasztalataim is a magyarországi szervezetekhez kötődnek. További a 2013. évi L. tv. által a szakembereknek előírt minősítések is innen származhatnak, így nem releváns más nemzetközi minősítés vagy oktatás mélyebb vizsgálata.

Oktatási, didaktikai fókuszú képzési profil, vagy támogatás nem jellemző ezen oktatásokra vagy képzésekre, ill. a minősítéseknél sem elvárt ilyen irányú mélyebb ismeret vagy gyakorlat. Általánosságban nincs egységesen koordinálva az információbiztonsági oktatás a

közigazgatásban, annak számos vetületével, ahogy arra már utaltam, munkaszervezetenként jelentős eltérések lehetnek az előírások értelmezésében. Továbbá a képesítés alapjaként nem szolgál oktatási, didaktikai felkészítés. Egyéb támogatás, például kommunikációs képességek fejlesztése vagy előkészített kiadványok nem állnak rendelkezésre. Így elképzelhető, hogy a képesített munkavállalók nem tudják hatékonyan átadni, meggyőzni az egyes szerepkörökben dolgozókat. Az oktatások megtartása esetleges, ezek ellenőrzése nem történik meg. Ahol megvalósul az oktatás, ott sincs egységes oktatásmódszertan vagy követelményrendszer. Az oktatások kapcsán jellemzően nem valósulnak meg mérések (jelenállapot, hatékonyság), vagy nem alátámasztott, hogy a kockázatokra reagálva, azzal arányosan kerülnek kialakításra. Az egyes elszórt mérések esetiek, nem összehasonlíthatóak, idősorosan nem állnak rendelkezésre. Így egy ideális szervezetben, ahol megvalósulnak az oktatások, erről igazoló feljegyzések keletkeznek, és még ezt követően a tananyag elsajátításának mértékéről, az oktatás hatékonyságáról gyors és negyedéves mérés is elvégzésre kerül, ott sem vethető össze ez a teljes populációval, más munkaszervezetekkel - azaz szigetszerű marad, nem biztosít valódi fejlődést. Az oktatás megértése alatt itt a tananyag elsajátításának mértékét, sikerességét értem. Mindezek alapján azt is állítom, hogy megfelelő felkészítéssel, oktatással növelhető a tudatossági szint, a tudatosság gyakorlatba való átültetése. Ilyen módon már ki is rajzolódik az összefüggés, miszerint a kiberbiztonsági szint (és tudatossági szint) fejleszthető oktatás segítségével.

1.2. KITŰZÖTT KUTATÁSI CÉLOK

A kutatási munka kezdetén az alábbi kérdések vetődtek fel bennem:

- A magyar szakirodalomban milyen hangsúlyt kap az információbiztonság?
- Ezen kérdések milyen mértékben valósulnak meg a gyakorlatban?
- Vannak-e hiányosságai a információbiztonsági képzéseknek hazánkban?
- Milyen mértékben foglalkoznak ezen kérdéssel a külföldi szakirodalomban, milyen gyakorlati tapasztalatokat hasznosíthatnánk azokból?
- Milyen megfontolás alapján legyen szervezve a különböző alapvégzettségű szakemberek képzése?
- Milyen befolyásoló tényezőkkel számolhatunk még az oktatás során?
- Milyen tényezők segíthetik elő, hogy a gyakorlatba átültetődjön a tudás – például, hogy helyesen járjon el az egyén egy stresszszituációban?
- Milyen mérések szükségesek előzetesen, ill. utólagosan?
- Milyen viselkedési normák szükségesek az elsajátítás során?
- Melyek az információbiztonsági képzések hatékonyságának, ill. annak mérésének kérdései?
- Milyen megfontolás alapján legyen szervezve a különböző alapvégzettségű munkavállalók képzése?

A kutatási kérdéseim ezek alapján:

- Szükség van mérésekre?
- Szükség van folyamatos kontrollra?
- Szükség van-e oktatásra, s ha igen, milyen módszerekkel, eszközökkel és milyen gyakorisággal?
- Hogyan lehet kiértékelni a képzések hatékonyságát?
- Betartják-e az emberek a szabályokat (pl. jelentési kötelezettség)?
- Milyen indikátorok mérhetők ezen kérdésekben?
- Mi a szabálybetartási és -szegési motiváció (mi motiválja az egyént szabálybetartási viselkedésében vagy szabályzatszegés elkövetésében)?
- Milyen oktatási modellek és csatornák állnak ehhez rendelkezésre?
- A szabályozás megtervezésének, kialakításának és bevezetésének folyamata hogyan befolyásolja a szabályzat betarthatóságát és elfogadottságát?
- A szabályozás elfogadása (a szabályzat megismerése, megértése és annak megfelelő szabálykövetés) milyen tényezőkre vezethető vissza, hogyan befolyásolható?

- Milyen tényezők befolyásolják a tanulási és felejtési görbét, s melyek az oktatás rendszerességét befolyásoló további tényezők?

Ezen kérdések mentén megfogalmaztam hipotéziseimet:

H1: Az információbiztonsági tudatossági szintjének tekintetében a magyar közigazgatás területén nem tapasztalható lemaradás a magyar üzleti szférával összehasonlítva

H2: Az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest

H3: Az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető.

A jövőben vizsgálható, hogy az e-learning oktatás hatékonyabbá tehető-e, ha annak egyéb e-learningben elérhető, tágabban értelmezett, disszertációmban bemutatott, de általam nem alkalmazott funkciói is alkalmazásra kerülnek.
Disszertációmban a soft tényezők közül csak a bemutatott emberi tényezőket vizsgáltam, ugyanakkor számos más soft tényezővel és számos más elmélettel nem volt lehetőségem a terjedelmi korlátok miatt foglalkozni. Azonban egy jövőbeli kutatás tárgyát képezheti ezek vizsgálata: az elégedettség és motiváció, a stressz hatása az információbiztonságra, a felhasználói tudatosság érettségi modellje és felhasználási lehetőségei, az elfogadás, a kulturális befolyásoló tényezők, az elrettentő szankciók eredményessége, a személyes oktatási preferenciák figyelembevételének lehetőségei, a szervezeti tudásmenedzsment jelentette kihívások.
Mivel disszertációmban a hard tényezők közül csak szabályzatokkal foglalkoztam, lehetőség lenne a kutatást kiterjeszteni a kapcsolódó szabályzatokra és a szervezeti politika egyéb elemeire, etikai kódexre, fegyelmi szabályzatra stb., amelyek külön-külön is egy-egy kutatás tárgyát képezhetik. Továbbá annak vizsgálata, hogy a szabályozás, a szabályzatalkotás folyamata, annak optimalizálása, a stakeholderek, felhasználók bevonása milyen eredményeket hozhatna a szabálykövetési hajlandóságban, vagy a folyamatok jobb megértése és jobb feltérképezése révén milyen input információkat képes szolgáltatni a compliance distance érzékeléséhez. Valamint ha a jelenléti oktatás keretében kapott információkat bemeneti információként felhasználva alkalmazzuk a compliance distance módszertanra, ennek eredményességét lenne lehetséges vizsgálni.

2. SZAKIRODALMI ÁTTEKINTÉS

Az EU Safer Internet Program (EU SIP) keretén belül 2010-ben vettem részt az első olyan oktatáson, amelyet a későbbi önkéntes oktatóknak tartott Krasznay Csaba. Az EU SIP önkéntes oktatójaként felmerült bennem a kérdés, hogyan lehet felkelteni, fenntartani az érdeklődést, és hogyan lehet meggyőzni a szabálykövetésről bárkit is. Ugyanakkor később az NKE EIV képzésbe bekapcsolódó oktatóként is hiányt éreztem abban, hogy ezekre a kérdésekre nem kaptam választ a magyar szakirodalomból; legfeljebb megfigyelések, beszámolók voltak elérhetőek. Így a nemzetközi szakirodalom felé fordult figyelmem, és szisztematikusan elkezdtem feltérképezni azokat a határterületeket, amelyek választ adhatnak erre a nem tisztán információbiztonsági kérdésre. Ezen széles spektrumú nemzetközi szakirodalmi áttekintés során összességében több mint ezer, részben információbiztonsággal, igazából annak számos különböző megközelítésével, aspektusával foglalkozó tudományos cikket néztem át. Kifejezett célom volt megérteni azokat a mozgatórugókat, hogyan lehet elérni, hogy egy adott személy vagy csoport a kapott (új) ismeretek szerint járjon el, azokat a gyakorlatba ültesse; illetve hogyan elhelyezhetőek valamilyen képzési formával azok a figyelemfelhívó jelzőtáblák, bizonyos eseménysort kiváltó (trigger) pontok, amelyek észlelése esetén a felhasználói viselkedés a megfelelő eseménysort követi.

2.1. AZ INFORMÁCIÓBIZTONSÁG FOGALMI MEGKÖZELÍTÉSE, VALAMINT SZABÁLYOZÁSI HÁTTERE

Ahogy arra Muha, Krasznay (2014) (*Az elektronikus információs rendszerek biztonságának menedzselése*) könyvében is rámutat, számos oka van, hogy miért védjük az adatainkat és az információkat. Ennek a jogszabályi kötelezettség, az egyéni, vállalati vagy nemzeti érdek mellett sokféle oka lehet. Az emberi viselkedést számtalan összetevő vezérli. És ahogy Muha, Krasznay is bemutatja, részletes, szerepkörre szabott oktatás, képzés szükséges, amely a munkaszervezésben kell, hogy megvalósuljon. Azaz ezen leírásokat létre kell hozni, és kellő részletességgel, már a munkaszerződéstől kezdődően kell dokumentálni (Komor, Nagy In: Muha, 2000). Ugyanakkor ezen általános törekvések konfliktusba kerülnek, mert egyrészről "gyorsan" és "olcsón" adjuk át a tudást – azaz a leírás legyen rövid és közérthető, gyorsan alkalmazható –, miközben a munkafolyamataink, hétköznapi életünk és a minket körbevevő informatikai környezet egyre bonyolultabb. (Például kevés ember lenne képes pontosan elmondani a titkosításnál alkalmazott kulcscserét stb.) Valamint a "jó", azaz könnyen alkalmazható, megfelelő színvonalú tudás átadása is elvárás. Ahogy a későbbiekben is bemutatom, disszertációmban többek között erre is keresem a választ: Hogyan lehetséges a megfelelő, kockázatokkal arányosan meghatározott, szerepkör alapú tudás átültetése a gyakorlatba, viselkedésbe? A kockázatok felmérését, meghatározását követően szükséges azok rangsorolása hatás és valószínűség szerint. (Som, 2014)

Kockázat: "Egy vállalat, szervezet számára kockázatot jelentenek azok a potenciálisan bekövetkező külső és belső események, zavarok, amelyek következtében veszélybe kerül a vevői, ügyféligények kielégítése vagy bármely (vállalati) érintett (stake- és stockholder) biztonsága. Leegyszerűsítve a kockázat alatt bizonytalan események negatív hatásait értjük." (Michelberger, 2020)

László (2014) így fogalmaz: "A kockázat információhiányt jelöl. IT kockázat megközelítésmódjából kockázat (R) a fenyegetettség mértéke, amely egy fenyegetés bekövetkezési gyakoriságának (bekövetkezési valószínűségének, W) és az ez által okozott kár nagyságának/súlyosságának (K) a függvénye. Matematikai megközelítésben: $R = W \times K$."

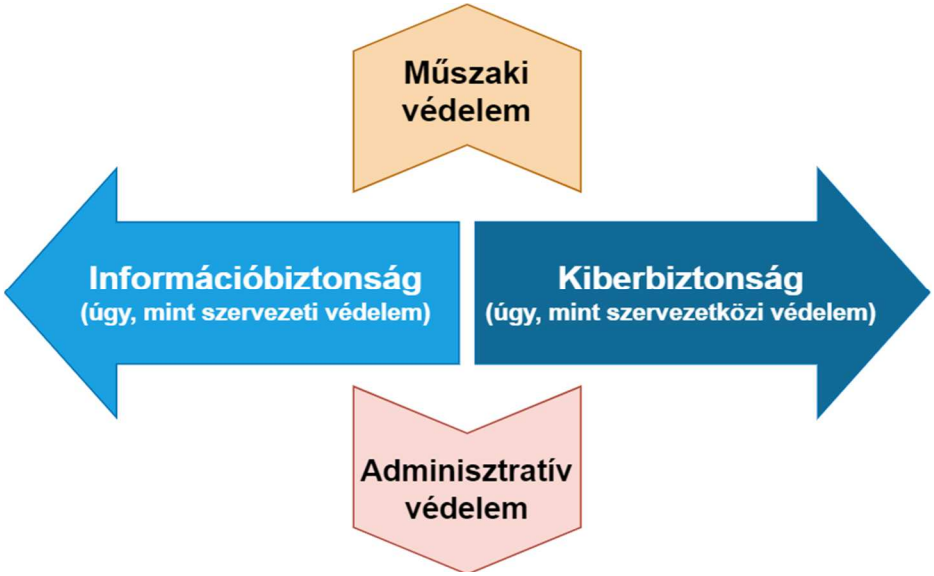
Információbiztonság: az elektronikus információs rendszer olyan állapota, amelyben annak védelme az elektronikus információs rendszerben kezelt adatok bizalmassága, sértetlensége és rendelkezésre állása, valamint az elektronikus információs rendszer elemeinek sértetlensége és rendelkezésre állása szempontjából zárt, teljes körű, folytonos és a kockázatokkal arányos. (Muha, Krasznay, 2014; Muha 2007; Muha 2008)

Ugyanakkor Bederna, Rajnai, Szádeczky, (2021) is az üzleti érdekek és célok kockázatokhoz való igazítása, az incidensekből való tanulságok levonása mellett érvel, sőt a balanced scorecard (Kaplan & Norton, 1992, in Bederna, Rajnai, Szádeczky, 2021) fogalmát, mint a kockázatok időben érzékeléséhez szükséges tényezőt említi.

Kiberbiztonság: a kibertérben létező kockázatok kezelésére alkalmazható politikai, jogi, gazdasági, oktatási és tudatosságnövelő, valamint technikai eszközök folyamatos és tervszerű alkalmazása, amelyek a kibertérben létező kockázatok elfogadható szintjét biztosítva a kiberteret megbízható környezetté alakítják a társadalmi és gazdasági folyamatok zavartalan működéséhez és működtetéséhez (Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat In: Muha, Krasznay 2014;)

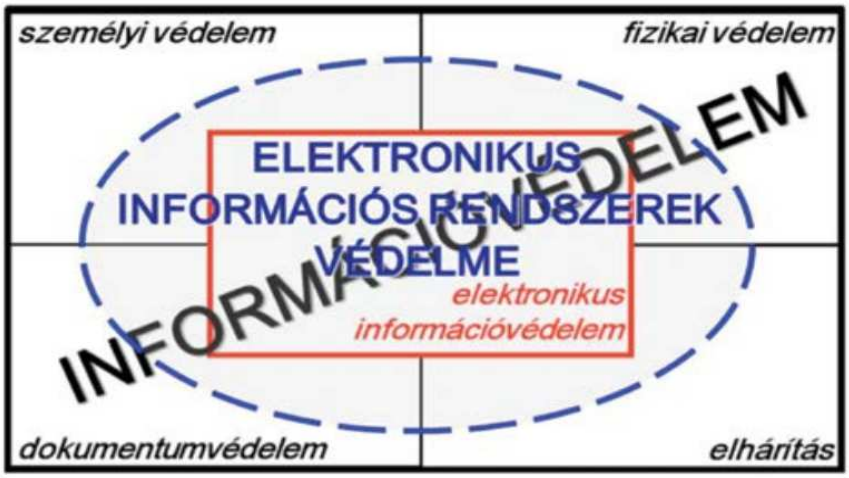
A hazai és nemzetközi szakirodalomban is gyakran szinonimaként használják az információbiztonsági és kiberbiztonsági kifejezéseket. Ez véleményem szerint alapvetően nem hiba, de mégis érdemes a két fogalmat elkülöníteni.

Az alábbi ábra jól mutatja, hogy több dimenziója van ezen fogalmaknak. Tehát a kiberbiztonság inkább nemzeti vagy szervezetközi szinten értelmezhető, míg az információbiztonság inkább szervezeti és egyéni szinten. (Muha, Krasznay, 2004) Ebbe beletartozik az informatikai biztonság és általában minden, ami az információ védelméhez kapcsolódhat, így a fizikai biztonság stb. is. A védelem érdekében alkalmazott megoldások vonatkozásában pedig az adminisztratív terület az, amely inkább szabályozásra, ki nem kényszeríthető kontrollokra vonatkozik; míg a műszaki védelem az, amely jellemzően valamilyen beállított, kikényszerített kontrollra vagy beállításra vonatkozik, vagy ez értendő alatta.

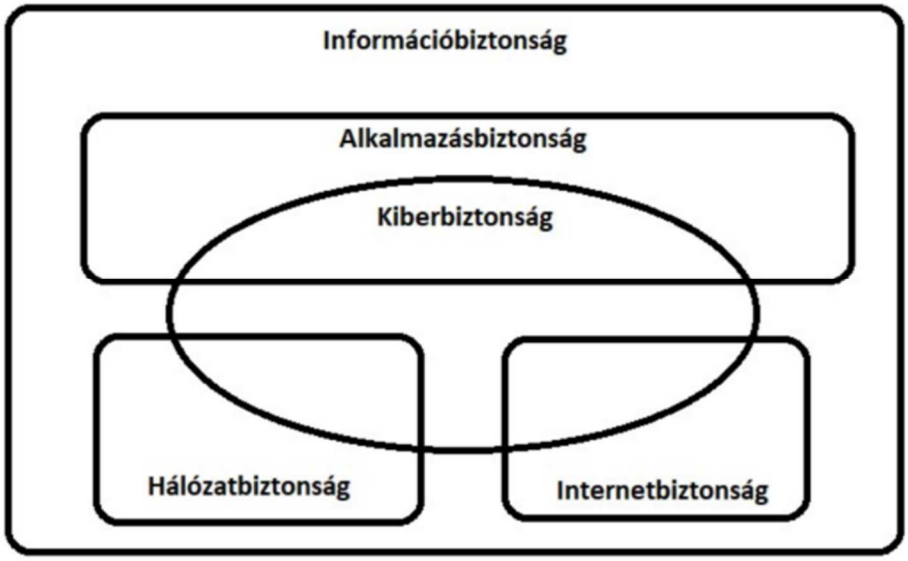


1. ábra: Az információbiztonság dimenziói, forrás: Krasznay (Elhangzott: Krasznay Csaba (NKE): Információbiztonság vs. kiberbiztonság, 5. Magyar Jövő Internet Konferencia, Okos város a célkeresztben, 2018. november 28., a Tudomány hónapja keretében)

Ugyanakkor tapasztalható, hogy „Divattá vált a kiber előtaggal megjelölni bármit, ami az internethez, az elektronikus információs rendszerekhez kötődik, ... „Tulajdonképpen mindenre, ami az internethez, az elektronikus információs rendszerekhez kötődik, de különösen ott, ahol valamilyen fenyegetés tárgya vagy eszköze az internet, az elektronikus információs rendszer.” (Muha, Krasznay, 2014; Muha, 2012). Azaz a kiberbiztonság, a kiber védelem, ahogy a 2. számú ábrán látható egy nagyobb információbiztonságnak a részhalmaza, ahol az információbiztonság nem csak a kiber, azaz a számítógépesített rendszerekre terjed ki. Az információbiztonság mindenképpen egy nagyobb halmaz, amibe beletartozik például, de nem kizárólag az adatbiztonság, a hálózatbiztonság és a nem elektronikus adatok védelme is.



3. ábra: Az elektronikus információvédelem és az információbiztonság kapcsolata, forrás: Muha 2007 In: Muha, Krasznay 2014;



2. ábra: : A fogalmak egymásra épülésének rendszere (Tarján 2020, készült az ISO/IEC 27032:2012 szabvány 11. oldalán található hasonló tartalmú ábra nyomán)

Ugyan ezt a kérdéskört szemlélteti Tarján (2020) a 3. számú ábrán. A 3. számú ábrán az látható, hogy a halmazrendszer univerzuma az információbiztonság, amelynek több, egymást részben akár metsző részhalmaza lehetséges, vélhetőleg az ábrán szemléltetettnél több.

2.1.1. AZ INFORMÁCIÓBIZTONSÁG FŐBB FOGALMAINAK TISZTÁZÁSA

A fentiekben adott definíciókon túl az alábbiakban csak pár gyakori tévedés és lehetséges félreértés elkerülése érdekében kívánom pontosítani az információbiztonság és -tudatosság kapcsán használt fogalmakat, kifejezéseket.

Az információbiztonság nem egyenlő az informatikai biztonsággal. Míg az informatikai biztonság jellemzően az elektronikus (számítógépes) rendszerek biztonságára fókuszál, addig az információbiztonság ezen túlmutat, az információ minden lehetséges megjelenési formáját, annak bizalmassági, sértetlenségi és rendelkezésre állási szempontjait veszi figyelembe.

A kiberbiztonság, ahogy fentebb már írtam, inkább globálisabb értelemben használandó vagy más értelmezésben a számítógépesített, elektronikus rendszerek vonatkozásában.

Mindezeken kívül a security awareness információbiztonsági tudatosság fogalmát is használom disszertációmban, amely azonban szintén további pontosításra szorulhat.

Tekintsük végig a szabálykövetési lehetőségeket és fokozatokat az egyén információbiztonsági tudatossági érettsége alapján:

- Nem tud az információbiztonsági szabályzatról, annak elérhetőségéről, így annak betartására sem képes, mert nem rendelkezik megfelelő mennyiségű és minőségű ismerettel.
- Érintőlegesen tud az információbiztonsági szabályzatról vagy munkaszervezeti elvárásokról. Pontos és mélységi ismerete nincs, a szabályzatot nem olvasta, vagy olvasta, de nem értette, saját munkafolyamataiban nem tudta alkalmazni, így annak betartására sem képes, mert nem rendelkezik megfelelő mennyiségű és minőségű ismerettel.
- Tud az információbiztonsági szabályzatról, számára annak elérhetősége is ismert, szándéka és törekvése van (belső motiváció), hogy betartsa, de nem érti pontosan, saját munkafolyamatait nehezíti, annak előírásaival részlegesen vagy teljesen nem ért egyet. A "hatékony" munkavégzés, csoportnyomás, kongruenciasértés vagy egyéb okokból kifolyólag nem minden esetben tartja be, vagy nem tudja minden esetben alkalmazni a szabályzatot.

A fenti és azt követő lehetséges szcenáriók mellett más kombináció is elképzelhető, de a felsorolás nagyságrendileg a következővel kell, hogy záruljon:

- Tud a információbiztonsági szabályzatról, elérhetősége is ismert számára, olyan oktatásban (vagy tréningben) részesült, amely révén saját munkafolyamataira azt alkalmazni tudja. Optimális esetben a környezetében lévő munkavállalók is hasonló attitűddel rendelkeznek, így a csoportnorma támogató, belső információbiztonsági tudása kongruens. Tehát mind a munkaszervezetben, mind a magánéletben megvan a lehetséges kockázatokkal arányos mértékű tudása. Mindezen tudást a gyakorlatban is képes alkalmazni, elsősorban belső meggyőződéstől vezérelve.

Az *információbiztonsági oktatás* vagy *tréning* kifejezések között értelmezésem szerint az a különbség, hogy megvalósul-e a gyakorlatba ültetéshez szükséges támogatás. A Magyar értelmező kéziszótárban az alábbi meghatározások szerepelnek.

oktat, ts ige 1. (t. n. is) hiv Tanít vkit vmire. A jóra oktatja; az iskola oktat és nevel. 2. pejor Leckéztet. [←ok]

oktatás, fn hiv 1. vál Az a cselekvés, tény, hogy vki(ke)t oktatnak. 2. A tanítás szervezett formája. Iskolai oktatás.
képzés, fn 1. Az a folyamat, tény, hogy vmit képeznek, alkotnak. 2. (Meghatározott irányú) oktatás, nevelés.

képez, ts ige 1. Vmire, kül. vmely szakmára, hivatásra tanítással, gyakoroltatással felkészít. képezi magát: tanul, művelődik. | Kiképez vmivé, vmire.

tréning, fn 1. Sp kiv Edzés. 2. (Elő)gyakorlat, gyakorlás. tréningje van vmiben: gyakorlata van benne. | <Munkahelyen, (felsőfokú) tanintézetben:> a személyiség alaposabb megismerését, es. formálását célzó gyakorlat(ok sorozata). (Magyar értelmező kéziszótár, 2014)

Disszertációm szempontjából az alkalmazott szakkifejezések vonatkozásában ennyi elegendő. A releváns nemzetközi szervezetek, ajánlások, gyakorlatok áttekintése után azt gondolom, hogy a széles szakirodalmi áttekintés, alapfogalmak számos definíciója nem mutat túl, nem tesz hozzá többet érdemben a fentiekhez.
Számos nemzetközi szervezet információbiztonsági oktató, tanúsított anyagaiban helyet kap a információbiztonsági oktatás, tudatosság. Azonban annak kibontása, hogy az oktatásból hogyan legyen szabálykövetés kérdése – a gyakorlatban önként történő alkalmazás hogyan valósuljon meg – hiányzik. A széles spektrumú nemzetközi szakirodalmi áttekintése során ezen kérdésekre is kerestem a választ.
Az információs rendszerek körbeveszik hétköznapi életünket, annak minden általánosan igénybe vett szolgáltatását. Információs rendszerek állnak a jellemző és elterjedt közüzemi szolgáltatások

(víz, gáz, áram, csatorna, internet, televízió és egyéb műsorszóró szolgáltatások) mögött. Ezen szolgáltatások használata annyira természetes, hogy a hétköznapi életben a felhasználó nem is tekint rá úgy, mint kritikus infrastruktúrára. Elmosódik a határ, összeolvad a fizikai és virtuális világ. Erre számos példát lehetne említeni; a hétköznapi élet, mindennapi rutin részeként számos hagyományos és/vagy információs eszközt és mögöttük számos információs rendszert veszünk igénybe. Ezen változások „szinte észrevétlenül" következnek be, elterjednek. Valamint fejlődnek és változnak is. Természetesen a változás érzékelhető és tetten érhető, ha azt kellő időtávlatban vizsgáljuk. Itt a bevezetésben egyetlen példát kívánok szerepeltetni. Saját tapasztalataim és megfigyeléseim alapján az 1990-es években kezdtek elterjedni Magyarországon a személyi számítógépek. Egyes egyetemeken Silicon Grafich számítógépek is elérhetőek voltak. Ezek az eszközök nem voltak kifejezetten hordozhatóak, de semmiképpen sem útközben vagy menet közben használhatóak. Természetesen a diákok egymást meglátogatva floppy lemezeken már tudtak programokat cserélgetni. Az internet magán, otthoni használata az évtized első felében alacsonynak tekinthető. 2013-as megfigyeléseim alapján az általános iskola 4. és 5. osztályos korosztályában elterjedt (50%-nál magasabb) az okos eszközök használata és a közösségi hálózatokon való (önálló vagy szülővel közös) jelenlét. 2017-es megfigyeléseim alapján pedig már azt tapasztalom, hogy 3. és 4. osztályban jelenik meg az előbbiekben bemutatott magas penetráció. Ezeket az EU Safer Internet program oktatójaként, illetve egyéb oktatások alkalmával figyeltem meg.

Dolgozatomnak nem tárgya ezen okozatok okainak feltárása, például a nem kizárólag könnyebben és olcsóbban hozzáférhető eszközök, a könnyebben és olcsóbban hozzáférhető infrastruktúra és szolgáltatások, a csoportnyomás („Anyu, másnak is ilyenje van az oviban!") vizsgálata. Dolgozatomban a változást mint tényt, axiómát kezelem. Vizsgálatom inkább a változás társadalmi, törvényi, szabályozási, és legfőképp oktatási, tudatossági területére fókuszál.

Azt kijelenthetjük, hogy a változás érzékelhető és megtörténik. A változás örök. „Hérakleitosz azt mondja valahol, hogy minden mozgásban van, és semmi sem marad változatlan, és a folyó áramlásához hasonlítva a létezőket, azt mondja, hogy nem léphetsz kétszer ugyanabba a folyóba." (Platón) Azonban nemcsak a változás maga vizsgálandó, hanem a változás sebessége is, amely szintén változik időben. A Központi Statisztikai Hivatal (KSH) weblapján elérhető információk szerint is „Az egyéni IKT eszköz használat mutatói életkor szerint" növekedést mutatnak. (KSH, 2019)

Szádeczky (2018) áttekinti az IT biztonság szabályozását. Szerinte a munkaszervezetek tekintetében az üzleti, informatikai és információbiztonsági stratégiai kérdéseket egységesen és magas szinten szükséges kezelni, és számos kockázatra, azok felmérésére és értékelésére ad

konkrét példát. Ugyanakkor rámutatva, hogy a gyors ütemű változások, a jogi szabályozás és az információbiztonsági védelmi mechanizmusok nem mindig fognak tökéletesen illeszkedni, az ehhez szükséges emberi faktor nem automatizálható.

Az információs eszközök használata tehát már fiatal kortól a hétköznapok része lehet. Ez azonban felvet bizonyos kérdéseket: Honnan sajátítja el az adott személy a megfelelő használatot? Mit tekintünk megfelelő használatnak? 50 évvel ezelőtt egy vidéki vagy városi gyermek megfelelő eszközhasználata jól tetten érhető volt fizikai tekintetben. Egészséges maradt, nem esett le, nem vágta el semmilyen testrészét stb. Jelenleg ez sokkal bonyolultabb és összetettebb kérdés, mármint annak megállapítása, hogy megfelelően használja-e mondjuk egy (a példánál maradva) 10 éves gyermek a közösségi hálózatot és/vagy információs (okos) eszközét.
Mivel meggyőzni nagyon nehéz bárkit, így tudományos dolgozatom tárgya annak vizsgálata, hogyan lehet valakit olyan információk birtokába juttatni, amelyből adott helyzetben már megfelelő, önálló döntések meghozatalára lesz képes. Ez pedig kifejezetten az információs rendszerek megfelelő, tudatos használata révén lehetséges. Ezért ezen tudatossági szint mérése, értékelése és fejlesztése az, ami az elmúlt években vizsgálódásaim fókuszában van.

Ugyanakkor azt tapasztaltam, hogy a szabályozás és kockázatok puszta elmondásával vagy elolvastatásával, a helyes gyakorlat puszta bemutatásával nem győzhetőek meg minden esetben az emberek. Ez az ellentét vezetett el oda, hogy kidolgozzam oktatási módszertanom, amely választ és megoldást ad arra, hogyan lehetséges új információ bevitele kongruens módon, ami a későbbi viselkedés, döntéshozatal alapját képezheti.
Voltaképpen tehát, amikor információbiztonsági tudatosságról, “security awareness”-ről beszélünk, akkor a megszerzett vagy oktatott tudás alkalmazását lenne szükséges ez alatt érteni, a szabálykövetési hajlandóságot. Sajnos mind a magyar, mind a nemzetközi szakirodalomban még kibontakozóban van ez a megközelítés. Igaz ez a legnagyobb szervezetek által nyújtott, tanúsított (információbiztonsági) képzésekhez kapcsolódó tananyagokra is. Ez alól egyedül talán az ISC^2 szervezet CISSP tananyaga kivétel. Természetesen a szabályalkalmazásnak is számos forrása és megközelítése lehet, ahogy azt disszertációmban is több oldalról közelítem meg: honnan szerzi az ismereteit, csak írott szabályzat áll-e rendelkezésére, milyen csatornán kapott képzést, milyen a munkaszervezetben a csoportnyomás, a kultúra, tud-e feltenni kérdéseket a saját munkafolyamataiban alkalmazandó szabályok alkalmazhatóságával kapcsolatban… és még lehetne folytatni. Az elérendő cél viszont az információbiztonsági tudatosság fejlesztésében nem lehet egyéb, mint hogy:

egyéni szinten

- megfelelő szerepkörre szabott információbiztonsági támogatást tudjon biztosítani az információbiztonsági szervezet,
- a kapott támogatást képes legyen olyan szinten megérteni, hogy a saját, releváns munkafolyamataiban azt alkalmazni tudja;

szervezeti szinten

- a szervezet a szabályzataival, oktatási tervével összhangban tudjon erőforrást allokálni a tudatosság fejlesztésére (kockázatfelmérés, OPDCA modell alkalmazása);

nemzeti szinten

- minél szélesebb körben képes legyen támogatást biztosítani,
- olyan lazán kötődő területeken is, mint a médiaműveletek, dezinformáció, fiatalok vagy időszak támogatása,
- alapvető oktatási folyamatokba épüljön be.

Tehát a szabályalkalmazás képessége az, ami végső soron elérendő cél. Természetesen ezen túlmenően is vannak még opcionális lehetőségek, hiszen a munkavállaló támogatásának bizonyos fokig javasolt túlnyúlnia a munkahely szigorú (logikai, fizikai) határain, részben a magánéleti területekre is javasolt kiterjednie. Egyetlen példával megvilágítva: A munkavállaló hazavisz olykor munkahelyi eszközöket. Ezek lehetnek BYOD vagy munkahelyi eszközök - mindez szempontunkból irreleváns. A munkavállaló tehát hazaviszi az adatokat, a "munkát", az adathordozót, használhatja a céges bankkártyát. A közösségi hálózaton érkező megtévesztési kísérleteket is praktikus, ha felismeri. Azaz nem választható el élesen a munkahelyi és a magánéleti terület. Más kutatók rámutatnak, hogy a kiberbűnözés és közösségi média, illetve minden olyan platform és terület, ahol lehetőség van kártékony kód terjesztésére, információszerzésre, zsarolóvírus vagy egyéb, nagy tömegekben végrehajtható anyagi vagy egyéb motivációból elkövetett haszonszerzésre, komoly kockázatként kezelendő. (Bányász, 2017) Ugyanakkor Bányász (2020) rámutat, hogy az elektronikus kognitív demokrácia, amely voltaképpen a közigazgatásba begyűrűzik a közösségi hálózatok révén, a visszacsatolás lehetősége. Mindezek azt támasztják alá, hogy a kérdést globálisabban, nemzeti szinten is érdemes vizsgálni, ugyanakkor ennek első és megfelelő lépcsőfoka lehet a közigazgatás.

Magyarországon a közigazgatáson keresztül nemzeti szinten lehetséges az információbiztonsági tudatosság emelése. Disszertációmban „nemzeti" szint alatt Magyarország országhatár és közigazgatás szerinti kiterjedését értem. Számos vetülete van, hogy miért fontos, szükséges az

információbiztonság fejlesztése: például az álhírek felismerése, a megtévesztő levelek felismerése, különböző csalási formák felismerése. Az álhírek, dezinformáció jelentette fenyegetés jelentős. Kovács és Krasznay (2017) szemléletesen bemutatja, hogy minden eddiginél nagyobb szerepet kaptak a "médiaműveletek" és az a törekvés, hogy külföldi államok, érdekek különböző – elsősorban informatikai (rendszereket felhasználó) – támadásokkal és médiaeszközökkel befolyásolják, befolyásolhatják akár a választások eredményét. Az érdemben befolyásoló tényezőkből az informatikai támadásokat és különböző médiaműveleteket rendezi kronológiai sorrendbe, és elemezi, hogyan lehettek hatással az elnökválasztásra, egy ország, a világ sorsára. Valamint számos lehetséges szcenáriót vizsgálva – főleg az elmúlt évtizedek történéseit tekintve – igen életszerű példákat hoz az információs hadviselésre. (Kovács, Krasznay, 2017). Kézzelfogható tény, hogy éves szinten ezres nagyságrendben jelennek meg dezinformációs, fakenews hírek kifejezetten nemzetközi politikát érintő kérdésekben; Az EU a https://euvsdisinfo.eu/ oldalon 2015-től dokumentálja ezeket, bár talán a teljesség igénye nélkül. Dolgozatomban ugyanakkor elsősorban nem a Magyarországi (mint országos, nemzeti szintű) szabályozási kérdéseket, hanem a munkaszervezetekben alkalmazott, alkalmazható szabályozási és egyéb kérdéseket vizsgálom. Meg kell említeni, hogy természetesen az egyes rétegek és nézőpontok, megközelítések nem választhatóak el hermetikusan, azok hatással vannak egymásra, akár nemzeti, akár közigazgatási, munkaszervezeti szinten vizsgáljuk, vagy teszünk javaslatot a fejlesztésre. Kovács (2017) így fogalmaz: "a felhasználóknak megfelelő biztonságtudatossággal kell vagy kellene rendelkeznie nemcsak a Facebook, hanem más közösségi médium használata során is". Számszerűen bemutatja azokat a változásokat, növekedéseket, amelyek szinte észrevétlenül történtek meg az elmúlt bő évtizedben. Szintén kiemeli az oktatás mint a legfontosabb, a legelső megtehető lépés fontosságát: "Az első ilyen védelmi intézkedés az oktatás és a képzés. Ez ugyanakkor az egyik legjobban és talán a leggyorsabban megtérülő befektetés a biztonság megteremtése érdekében, hiszen a felhasználók biztonságtudatosságának növelése egy egyszerű oktatással vagy rendszeresen ismétlődő képzéssel nagyban növelhető. Mivel a felhasználók jelentik minden rendszerben a biztonság leggyengébb láncszemét, értelemszerűen az ő felkészítésük és nem utolsósorban folyamatos képzésük ezen a területen nagyon gyorsan és nagyon látványosan hozhat eredményeket."

2.1.2. AZ INFORMÁCIÓBIZTONSÁG SZABÁLYOZÁSI KÉRDÉSEI

Az információbiztonsági politika és szabályzat kritikus szerepet játszik az információbiztonsági kultúra irányításában. A szervezetek számára fontos üzenet, hogy az információbiztonsági

szabályzat nélkülözhetetlen, de ha az alkalmazottak nem olvasták el vagy nem értették meg, akkor az nem lesz hatékony a viselkedésük irányításában, a szabályzat betartásával kapcsolatos hozzáállásuk befolyásolásában vagy az erős információbiztonsági kultúra előmozdításában. Minden harmadik szervezetből legalább egyben még mindig nincs írásbeli információbiztonsági vagy adatvédelmi szabályzat, és közel 24%-uknak nincs elfogadható használati politikája (acceptable usage policy) (Protiviti, 2014). Az információbiztonság megsértésének 2015. évi felmérése (2015 Information Security Breaches Survey – ISBS, 2015) azt jelzi, hogy „azoknak a vállalatoknak a 72%-ában, amelyekben a biztonsági politikát nem értették meg, a személyzettel kapcsolatos biztonsági kihágások tapasztalhatóak (staff related breaches)". Ez nemcsak az információvédelem kockázatát hordozza magában, hanem jogi következményekkel is járhat, és végül olyan információbiztonsági kultúrát vonhat maga után, amely nem járul hozzá az információk védelméhez.

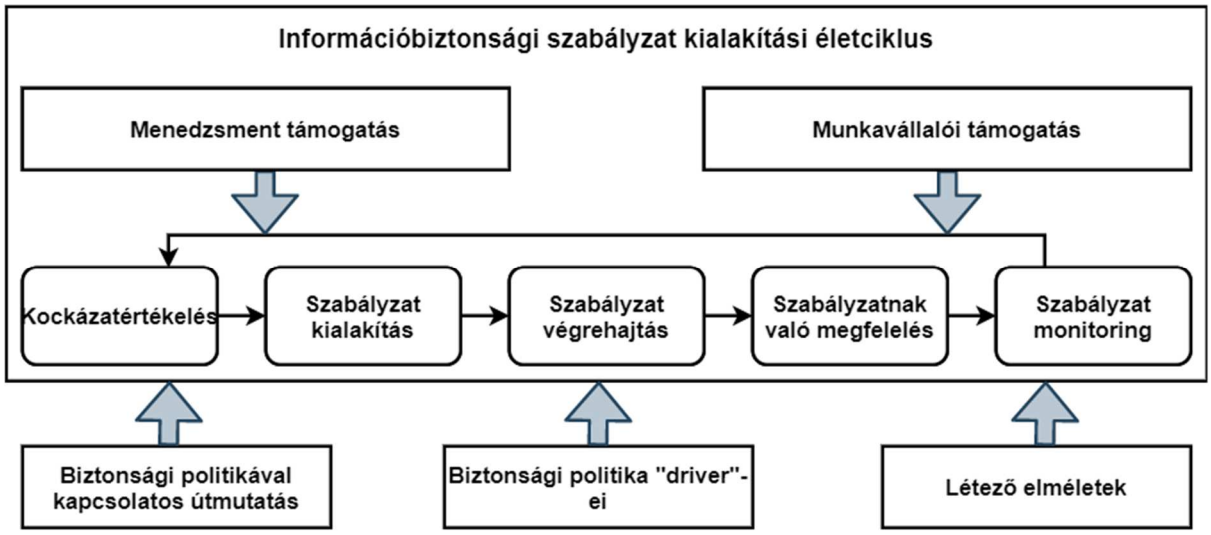
A nemzetközi szakirodalom vegyesen alkalmazza az információbiztonsági politika és szabályzat (ISP – information security policy és politics) kifejezéseket. Alapvetően az információbiztonsági politika a felső vezetés elköteleződését szimbolizálja, magas irányelveket, állításokat, célokat fogalmaz meg jellemzően röviden, 1-2 oldalban. Az információbiztonsági szabályzat vagy szabályzatok (információbiztonsági szabályozási környezet) egy vagy több szabályzatot jelentenek, amelyek mind terjedelemben, mind fókuszukban viszonylag nagy skálán mozoghatnak. Továbbá számos alacsonyabb rendű munkautasítást, szabványos működési eljárást (munkautasítás vagy SOP standard operating procedure) is magában foglalhatnak. Disszertációmban az információbiztonsági szabályozási környezetre és kapcsolódó dokumentumok egészére fogom alkalmazni (egyes számban) az *információbiztonsági szabályzat* kifejezést.

A szabályozási környezet, az információbiztonsági szabályzatok megléte, kidolgozottsága, karbantartása, életciklus-menedzsmentje és azok kommunikációja, oktatása rendkívül, kiemelkedően fontos. A szabályozási környezet egy vagy több szinten is készülhet, azonban tipikus jegyei általában a politika, a (magas) szabályozási környezet és esetenként a (alacsonyabb) munkautasítások felépítése. Tehát az információbiztonsági szabályzatok (információbiztonsági szabályozási környezet) körébe tartozik a politika, amely a felső vezetés elköteleződését (is) reprezentálja és egy vagy több információbiztonsági szabályzat, valamint alacsonyabb szintű dokumentumok. Az információbiztonsági szabályzatok kidolgozása azonban nem csupán a politika megfogalmazását és végrehajtását foglalja magában. Amennyiben a szervezetnek nem sikerül felismeri a biztonsági politika kidolgozásához szükséges különféle lépéseket, erőforrásokat, akkor fennáll annak a kockázata, hogy egy rosszul átgondolt, hiányos,

felesleges és irreleváns politikát dolgoz ki, amelyet a felhasználók nem fognak teljes mértékben támogatni; magasabb költség és erőforrás mellett fog kevesebb vagy elenyésző eredményt produkálni. A politikát a felső vezetés elköteleződésének, szimbólumának is tartják, tehát a politika alatt voltaképpen ilyen értelemben az információbiztonsági stratégia további, írott rövidítése is érthető. Így fontos, hogy az a menedzsment konszenzusaként jöjjön létre. Ugyanakkor számos körülmény jelentős befolyással lehet a szabályzat „sikerére": eljut-e az információ a célszemélyekhez, megértik-e, képesek-e betartani – a csoportnyomást, vezetői támogatást és a későbbiekben részletezett szempontokat mind összességében kell vizsgálni egy sikeres szabályozási környezet kiépítése során.

Váczi, Toth-Laufer, Szádeczky, (2020) is foglalkozik az információbiztonság emberi megközelítésével. A magyar és nemzetközi szakirodalom is látszólag egyetért abban, hogy a modern rendszerek ellenére rendkívül magas a humán kockázat. Azonban az igény ellenére nincs a kiberbiztonságban széles körű, széles körben elterjedt, az emberi kockázat mérésére alkalmas módszer, részben mert ennek mérése nehéz. A szerzők egy fuzzy modellt javasolnak a szervezeteknek, amelyekkel mérni tudják ezt a kockázatot, ha elegendő információval rendelkeznek a munkaerőről. A modell egy-egy konkrét fenyegetés esetén megkönnyítheti a konkrét fenyegetés megértését, amelyet például a minősített információk kiszivárogtatása jelenthet.

Stephen és Tuyikeze (2016) szerzők például egy fogalmi keretrendszert dolgoztak ki, amely felvázolja a hatékony információbiztonsági szabályzat kidolgozásához és végrehajtásához szükséges különféle konstrukciókat, amelyeket a biztonsági szakembereknek javasolt figyelembe venniük. A *(Information security policy development and implementation: The what, how and who*) tanulmányukban megfogalmazzák, hogy a szervezeti információs eszközök védelmének egyik fontos mechanizmusa a hatékony információbiztonsági szabályozási környezet kidolgozása és végrehajtása. Ehhez bemutatnak egy kulcskomponenst, amit az „Információbiztonsági politika fejlesztési életciklusa" néven jegyeznek az információbiztonsági szabályzat fejlesztésének életciklusaként (Information Security Policy Development Life Cycle" (ISPDLC).



4. ábra: Az információbiztonsági szabályzat lehetséges keretrendszere, az ISPDLC komponenssel, Forrás: Stephen és Tuyikeze (2016) alapján

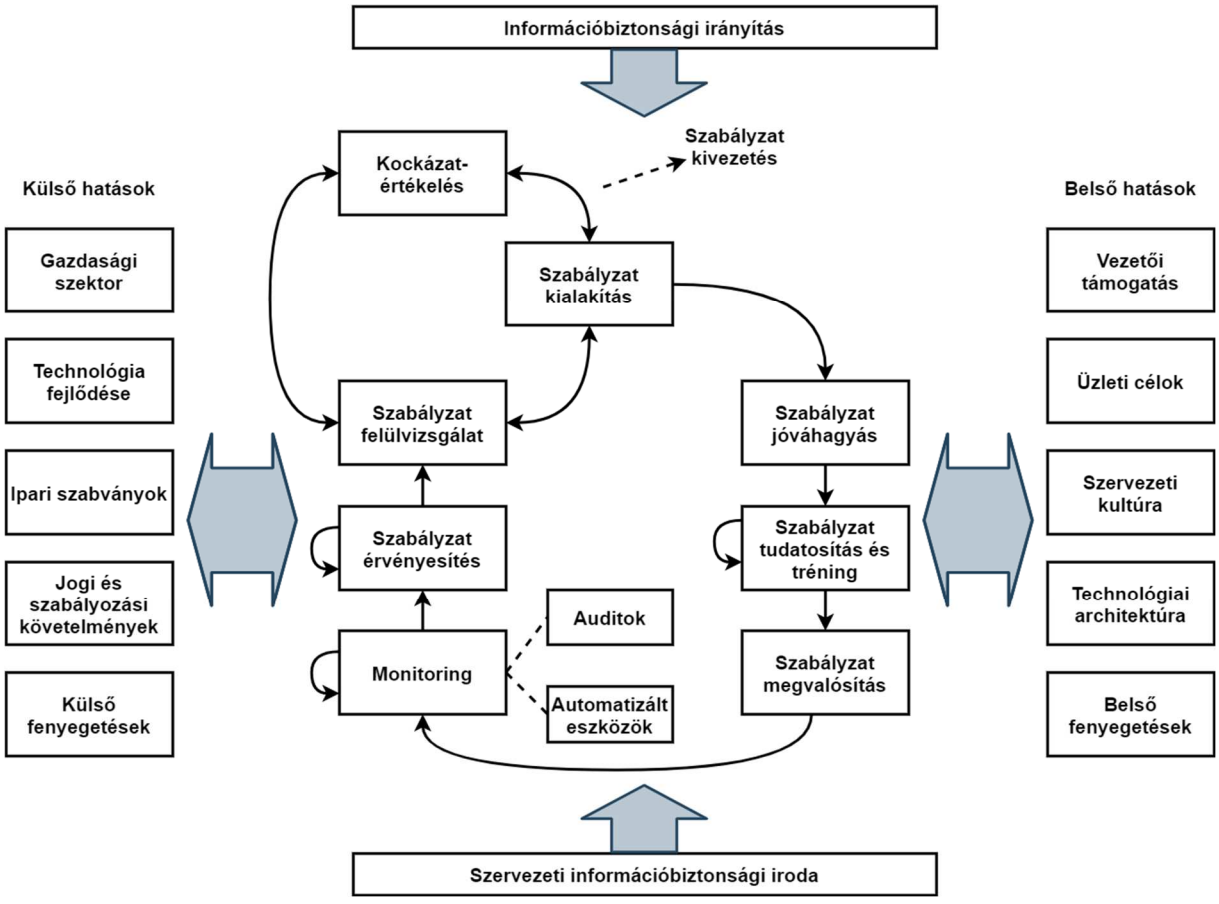
Így tehát megjelenik még egy fontos komponens, az időbeli sík, amely számos komponensre, a szabályzatok karbantartására, oktatásra, minden ciklikusan ismétlődő műveletre kiterjesztendő.
A szakirodalom számos meghatározást alkalmaz az információbiztonsági szabályzat definíciójára, céljára vonatkozólag. Hao és Wenli (2014) azt állítják, hogy az információbiztonsági szabályzatot a vezetés alkalmazza a munkavállalók által megengedett vagy tiltott viselkedés megkülönböztetésére, valamint a tiltott viselkedés esetén bekövetkező szankciókra. Ezzel a megközelítéssel szakmailag olyan szempontból maximálisan egyetértek, hogy az etikai kódexszel, HR-szabályzatokkal és fegyelmi szabályzatokkal koherens egészet kell alkotnia az információbiztonsági szabályzatnak. Másrészről az ISO / IEC 27002 (2013) kijelenti, hogy az információbiztonsági szabályzat célja irányítás és támogatás nyújtása a menedzsmentnek az üzleti követelményekkel és rendeletekkel összhangban az információbiztonság kezelésében. Amint azt a két meghatározás kiemeli, egyértelmű, hogy az információbiztonsági szabályzat jelentősen hozzájárul a szervezet hatékony információvédelméhez.

Simon (1957) ugyanakkor úgy fogalmaz, hogy az információbiztonsági szabályzat egy általános szabály (rendszer), amelyet egy szervezet határozott meg, hogy korlátozza a beosztottak mérlegelési jogkörét. Ezt a célt én talán úgy fogalmaznám át, hogy támogatást biztosítson a szervezet ahhoz, hogy megfelelően tudjon a munkavállaló döntést hozni. Ugyanakkor maga a szabályzat megléte ehhez sajnos kevés. Az információbiztonsági szabályzat kidolgozását mind külső, mind belső hatások vezérlik, amelyek nyomást gyakorolnak a szervezetre a szervezet információinak védelme érdekében. A belső fenyegetések közé tartoznak például az alkalmazottak, akik a szervezet információs kockázatát hordozzák, míg a külső fenyegetések közé tartoznak például a hackerek, kiberbűnözők, versenytársak. Ezen felül szükség van a szaporodó

kormányzati vagy uniós jogszabályi követelmények betartására. Ezek szervezetenként eltérőek lehetnek. A kockázatok felmérése és kiértékelése után képes a szervezet ezekről képet alkotni és cselekvési tervet kidolgozni.

Bayuk (2009) rámutat arra, hogy az információbiztonsági szabályzat kialakításának a felső vezetéssel kell kezdődnie. Ennek megfelelően az ügyvezetéstől származó irányelveket vagy magas szintű biztonsági politikákat a stratégiai szinttől a taktikai szintre terjesztik, ahol standardokba vagy iránymutatásokba (guidelines) ültetik át őket; végül eljárások formájában (procedures) terjesztik őket az operatív szintre.

Knappa és munkatársai (2009) mind tudományos, mind üzleti szempontok figyelembevételével készített szervezeti szintű folyamatábrát készített el az információbiztonsági szabályzat fejlesztési folyamatára (*Information security policy: An organizational-level process model*).



5. ábra: Egy átfogó információbiztonságiszabályzat-alkotási folyamat modell, forrás: Knappa et al. (2009) alapján

A 3. ábrán látható modell az információbiztonsági politika folyamatának egy gyakorlati alapú szemléletét tükrözi, amely megismételhető szervezeti folyamatként jelenik meg. Az ábra az általános információáramlást és a főbb interakciókat mutatja a kategóriák között (azaz

folyamatok) kiegészítve olyan külső, belső és egyéb tényezőkkel, amik a folyamatra hatnak. Az ilyen jellegű folyamatábrák adott szervezetre szabva alkalmasak lehetnek arra, hogy éves, időszakos és eseti változásokra reagálva a szervezet képes legyen a kockázatokkal arányos módon reagálni az információbiztonsági szintre.

A négy irányítási folyamat a politika felülvizsgálata (policy review), a kockázatértékelés (risk assessment), a politika kidolgozása (policy development) és a politika jóváhagyása (policy approval).

Azt gondolom, hogy a modell természetesen alkalmas lehet az információbiztonsági szabályzat fejlesztésére, habár nem tér ki időbeli és súlyozásbeli kérdésekre. Ugyanakkor egy idealizált szervezetben, ahol az érintettek (stakeholderek) tudják és teszik a dolgukat, ez jól alkalmazható modell lehet.

Az információbiztonsági szabályzattal kapcsolatos megállapítások

A nemzetközi és hazai szakirodalom általánosságban és túlnyomó részben egyetért azzal, hogy az információbiztonság legnagyobb veszélyét a gondatlan alkalmazottak jelentik, akik nem tartják be a szervezetek információbiztonsági szabályzatát és eljárásait. Más helyeken hasonló megfogalmazásban, de a gondatlanság kihangsúlyozása nélkül találkozunk ezzel a kijelentéssel.

A megállapítással nem teljes mértékben értek egyet, mivel féligazságot tartalmaz. Nem terjed ki arra a tényre, azokra az okokra, hogy vajon a gondatlanság miből fakad. Fel kell tenni ugyanis a kérdést: Vajon minden, maximális támogatást biztosított-e a munkaszervezet annak érdekében, hogy a szükséges típusú és mélységű tudás a munkavállaló eszközkészletébe beépüljön? Ennek hiányában ugyanis, bár a gyökérok változatlan, hiszen emberi mulasztásra vezethető vissza, ám akinek az oktatás, a megfelelő szabályozás kialakítása lett volna a feladata, az követhetett el mulasztást. Ilyen esetben tehát véleményem szerint a felelősség, illetve a mulasztás hibája nem elsősorban a végfelhasználót terheli. Amennyiben a munkavállalók nem ismerik a saját munkafolyamataikhoz releváns információbiztonsági szabályzatokat, az nem minden esetben és kizárólag az adott munkavállaló hibája.

A védelmi motivációs elmélet szerint (PMT), amely erőteljesen megmagyarázza a munkavállalók szándékát az információvédelem iránt, a munkavállalók viselkedése a fenyegetés-értékeléssel és a megküzdési értékeléssel kezdődik. (Anderson és Agarwal, 2010) A fenyegetés-értékelés egy fenyegető esemény kockázati szintjének személyes értékelése, amely a vélt kockázatból és az észlelt súlyosságból áll. Minél nagyobb az alkalmazottak biztonsági fenyegetése, annál szívesebben vesznek részt a biztonsági tevékenységekben. Az észlelt biztonsági fenyegetés pozitívan hat a vezetők azon szándékára is, hogy a szervezetben

alkalmazzák a biztonsági technológiákat. (Lee és Larsen, 2009) Sőt, az észlelt biztonsági fenyegetésről kiderül, hogy pozitívan befolyásolja a munkavállalók azon szándékát, hogy megfeleljenek az információbiztonsági szabályzatnak. (Ifinedo, 2011)

Woon et al. (2005) hangsúlyozza az információbiztonsági szabályzat észlelt relevanciáját. Ha az alkalmazottak az információbiztonsági szabályzatot nem látják relevánsnak és kellően naprakésznek munkájukhoz, akkor nem fogják betartani ezeket az irányelveket. Ugyanakkor azt is sugallja, hogy fontos például információbiztonsági oktatás vagy szóbeli meggyőzés révén biztosítani, hogy az alkalmazottak valóban használható tudást kapjanak az információbiztonsági intézkedésekről. Ezzel teljes mértékben egyetértek. Eddigi oktatási tapasztalataim érdekes kettősséget mutatnak a témában. Egyrészt az előadásokon levetített videók (audiovizuális ingerekkel bíró), kisfilmek felkeltik a résztvevők figyelmét, és a pár perces filmeket érdekesnek tartják; lelkesíti a résztvevőket, hogy nem csak frontális előadás van. Ugyanakkor, ha ezen kisfilmeket oktatás helyett vagy oktatásként, élő előadás helyett kapják kizárólag, akkor a tudás átültetése, a meggyőzési hatás, hogy az adott eljárásrendet tartsák be, elmarad.

Johnston eredményei például azt mutatják, hogy a válaszadás hatékonysága (response efficacy) jelentős hatással van az információbiztonsági szabályzat betartásának szándékára. Az információbiztonság megsértésének minimalizálása érdekében először fontos, hogy a szervezet információbiztonsági személyzete (is) tisztában legyen az információbiztonsági fenyegetésekkel (kockázatokkal), és tudja, hogyan kell reagálni ezekre. Másodszor, az információbiztonsági szabályzatnak világosnak és naprakésznek kell lennie, harmadszor pedig az alkalmazottaknak be kell tartaniuk az információbiztonsági szabályzatot. (Johnston and Warkentin, 2010)
Mindezt annyiban kívánom pontosítani, hogy 2. és 3. pont között el kell, hogy helyezkedjen az a fázis, amikor is megérti a munkavállaló, hogyan tudja a saját munkafolyamataiban alkalmazni az előírtakat.

Mikko et al. (2013) szerint a szankciók jelentős hatással vannak az információbiztonsági politikák tényleges betartására. Megfigyeléseim szerint a gyakorlatban ez azt jelenti, hogy a gyakorló szakembereknek látható módon meg kell határozniuk az információbiztonsági szabályzat megsértésének szankcióit. Itt azért fontos megjegyezni, hogy mit jelent a láthatóság. Ahogy kutatásaim részletesen bemutatom, ki fogok térni arra, hogy az információbiztonsági szabályzat (IBSZ) láthatósága, érthetősége több feltételrendszer összességeként értelmezhető; például kutatással is alátámasztom, hogy a közigazgatási munkaszervezetek jelentős részében nincs semmilyen, így szerepkör alapú kivonata sem az információbiztonsági szabályzatnak.
Különösen fontos, hogy az alkalmazottak elhiggyék, hogy az információbiztonsági szabályzat be nem tartását észlelik, és súlyos vagy arányos szankciókra kerül sor a nemmegfelelés miatt. Az

eredmények azt is sugallják, hogy a felderítésnek gyorsan meg kell történnie. (Mikko et al., 2013) Saját tapasztalataim alapján a felderítés és annak visszajelzése az adott munkavállaló felé két szempontból is fontos és szükséges. Egyrészt az adott munkavállaló kap egy jelzést és tanulási lehetőséget, rögzül a szabályzat előírása. Másrészről áttételesen a munkavállaló szűkebb csoportja is tudomást szerezhet arról, hogy az ilyen kisebb kihágások is feltárásra kerülnek, folyamatos a megfigyelés, érzékelés.

Emellett Ajzen (1991) megállapításai alapján az információbiztonsági szakembereknek tisztában kell lenniük azzal, hogy a társadalmi nyomásnak (szankciók: társadalmi visszautasítás) a felső vezetésnek, a munkavállaló közvetlen felettesének, munkatársainak és az információbiztonsági személyzetnek az információbiztonsági szabályzat betartásához való hozzáállása fontos az alkalmazottak információbiztonsági szabályzattal kapcsolatos attitűdje szempontjából. Ez összhangban áll azzal a megállapítással, hogy a szociális környezetnek hatása van az egyének viselkedésére.

Mikko et al. (2013) hangsúlyozza, hogy a verbális meggyőzés megteremtése és biztosítása érdekében a felső vezetésnek, a közvetlen felügyeletnek és az információbiztonsági alkalmazottaknak világosan és egyértelműen meg kell magyarázniuk az alkalmazottak számára az információbiztonsági politikák betartásának fontosságát.
Azaz véleményem szerint nem hagyható el teljes mértékben az online, élő oktatás, ahol az oktató visszacsatolást kaphat, az oktatott pedig kérdéseket tehet fel.

Ez a megállapítás kihatással lehet a szervezetek információbiztonsági oktatási stratégiájára. Mikko et al. (2013) megállapításával egyetértve, mindennek fényében a szervezeteknek különös figyelmet kell fordítaniuk a felső vezetés, az információbiztonsági felügyelők és az információbiztonsági személyzet képzésére annak érdekében, hogy hirdessék az információbiztonsági szabályzat betartásának fontosságát, és ezáltal társadalmi nyomást (social pressure – szociális nyomás) keltsenek az információbiztonsági szabályzat betartása felé.
Végül, az információbiztonsági szabályzat betartásának szándéka jelentős hatással van az információbiztonsági szabályzat tényleges betartására. A szándék egy olyan motivációs tényező, amely befolyásolja a viselkedést azáltal, hogy megmutatja, mennyire elszántan hajlandóak megpróbálni, és mekkora erőfeszítést fejtenek ki az emberek a magatartás végrehajtása érdekében. Minél erősebb a szándék az egyén részéről, hogy részt vegyen egy ilyen viselkedésben, annál valószínűbb, hogy végre fogja hajtani. (Mikko, 2007)

Az elrettentés fogalma több mint harminc éve a kriminológiai elméletek középpontjában áll. A terület egyik vezető elmélete Higgins (2005) szerint a GDT (general deterrence theory – általános elrettentés elmélete), amelyet eredetileg a bűnözői magatartás ellenőrzésére fejlesztettek

ki (controlling criminal behavior). A klasszikus elrettentési elmélet (classical deterrence theory) hagyományosan azt sugallja, hogy a büntetés bizonyossága, súlyossága és gyorsasága (celeritás – celerity) befolyásolja az emberek döntését abban, hogy bűncselekményt követnek el vagy sem. A bizonyosság azt jelenti, hogy az egyén úgy gondolja, hogy bűncselekményét felfedezik, míg a súlyosság azt jelenti, hogy szigorúan megbüntetik. A „celeritás" (gyorsaság, sebesség) arra utal, hogy a szankciók gyorsan bekövetkeznek. Straub (1990) úgy találta, hogy az információbiztonsági politika megsértése miatt kiszabott szankciók növelik a megfelelő információbiztonsági viselkedést. Személyes megfigyeléseim is egybevágnak ezzel; bár számszerűen nem tudom alátámasztani, de a munkavállalók az ilyen (büntetést megelőző) figyelmeztetések során úgy nyilatkoznak, hogy nem volt tudomásuk arról, hogy az adott cselekmény szabályzatba ütköző. Ugyanakkor ritka, hogy ugyanazon személyek ugyanazt a cselekményt, visszaélést újra elkövessék.

A büntetés önmagában azonban nem elegendő a munkavállaló nemkívánatos magatartásának megakadályozásához. Hiszen elképzelhető, hogy az a szabályzat, a szabály ismeretének vagy alkalmazási képességének hiányából fakad. D'Arcy és Herath (2011) azt javasolja, hogy további tényezőket is figyelembe kell venni a büntetés hatásának jobb megértése érdekében. Fontos megemlíteni, hogy a nem rosszindulatú biztonsági megsértéseket (non-malicious security violation) – azt a viselkedést, amelyet azon alkalmazottak folytatnak, akik nem tudatosan sértik meg a szervezet információbiztonsági szabályzatát, rosszindulatú károkozás szándéka nélkül cselekszenek – külön kell választani. (Guo et al., 2011)

A szankciók súlyossága befolyásolhatja az alkalmazottak információbiztonsági szabályzat megsértési szándékait. Ha az alkalmazottak érzékelik, hogy szigorú büntetésekre számíthatnak, amint az információbiztonsági szabályzat megsértésével rajtakapják őket, akkor kevésbé valószínű, hogy megsértik azt. Ugyanakkor D'Arcy et al. (2009) kimutatta, hogy a szankciók bizonyosságának nincs jelentős hatása. Tanulmánya szerint, amely a GDT-t alkalmazta az információbiztonsági visszaélés területén, a szankciók vegyes eredményeket mutattak. Ezt az információbiztonsági szakirodalmában Kankanhalli et al. (2003) is kimutatta. Az információbiztonsági szabályzat és a szankciók bizonyossága közötti nem szignifikáns kapcsolatot az magyarázza, hogy munkavállaló úgy érzi, ez a viselkedés megtehető, mert a kapcsolódó szankció nem súlyos. Ez elsősorban olyan tevékenységekre igaz, mint a jelszavak megosztása vagy a munkaállomás kijelentkezés nélkül való elhagyása. Ugyanakkor a nem szándékos, hanem ismerethiányból fakadó szabályzatsértésekre ez nem alkalmazható.

Végül Cheng et al. (2013) megállapításai azt sugallják, hogy a társadalmi nyomás szerepet játszik a munkavállalók információbiztonsági megsértési szándékában is. A kutatás negatív kapcsolatot

talált a szubjektív normák és az alkalmazottak információbiztonság-sértési szándékai között. Ez arra utal, hogy a közvetlen felügyelő, munkatárs, szervezet és család elvárásai nagy hatással vannak a munkavállalók szabályzat megsértési szándékára. Nemcsak mások elvárásai relevánsak az alkalmazottak információbiztonság-sértési szándékaira nézve, hanem a munkatársak észlelt viselkedése is.

Ezenkívül a társadalmi nyomás jelentős hatása azt vonja maga után, hogy a közvetlen felettesek, munkatársak elvárásai és viselkedése fontos szerepet játszanak a biztonsági magatartás befolyásolásában. Így a vezetők csökkenthetik a szabálysértési magatartást azáltal, hogy javítják szervezetük biztonsági légkörét. (Cheng et al., 2013) Véleményem szerint ide sorolható az információbiztonsági szabályzattal és előírásokkal kapcsolatos kommunikáció, a metakommunikáció, a személyes példamutatás és a szabályok betartásának megkövetelése is.

Más kutatások rámutatnak, hogy ha az ilyen biztonsági irányelveket nem kényszerítik ki (technikailag), akkor a legtöbb felhasználó elmulasztja végrehajtani azokat, különösen akkor, ha például szigorú jelszóigényekről van szó (Barra et al., 2010; McLeod et al., 2010; Furnell, 2011; Furnell, 2014). Ugyanakkor, ahogy disszertációmban rámutatok, ahhoz, hogy a kiadott szabályzatból oktatott vagy alkalmazott szabályzat legyen, lépéseket kell tenni. Amikor azonban a biztonsági irányelveket technológiailag kikényszerítik (például egy jelszó-ellenőrző szoftver és a zárolási házirend kombinációján keresztül), azok hatékonysága gyakran növekszik. (Kankanhalli, 2003) Sajnos a korlátozó jelszavas házirendek negatívan befolyásolhatják a munkavállalók termelékenységét (például az érvénytelen bejelentkezési kísérletek miatt a rendszerből történő kizárás végett elveszített idő miatt, az elfelejtett jelszavak visszaállításához szükséges idő miatt), és frusztrációt jelenthetnek a felhasználók számára, ha ezeket az irányelveket időben/energiában túlságosan magasnak ítélik meg (P. Inglesant, 2010).

Bulgurcu (2010) eredményei azt mutatják, hogy a szankciók súlyosságának növelése nem növeli jelentősen a válaszadók azon szándékát, hogy megfeleljenek az információbiztonsági politikának. Ezzel szemben az eredmények azt mutatják, hogy a kiszabott büntetés súlyossága negatívan befolyásolja az információbiztonsági politikák betartásának szándékát. Hasonló eredményeket talált Herath és Rao (2009), akik szerint a büntetés súlyossága negatív hatással volt a viselkedési szándékra. Ezzel kapcsolatos eredményeink magyarázata az, hogy a munkavállalók ellenállnak a túl szigorú természetű szankcióknak. Az eredmények azt sugallják, hogy minél szigorúbbak a szankciók, annál kevésbé valószínű, hogy a munkavállalók új biztonsági politikát követnek. A vállalatoknak ezt figyelembe kell venniük a szankciók meghatározásakor. Másrészről, az általános elrettentési elmélettel összhangban, a szankciók bizonyosságának és gyorsaságának növelése jelentősen növeli az új információbiztonsági szabályzat betartásának szándékát. Ez arra utal, hogy

a vállalatoknak javasolt kommunikálni, hogy az új biztonsági politikák be nem tartása gyors szankciókat eredményez, de nem feltétlenül szigorú szankciókat. Tapasztalataim is alátámasztják ezt az elméletet, azaz a gyors, de finom figyelmeztetés megfigyeléseim szerint a legtöbb esetben pontosan és hatékonyan éri el a célját.

Paananen et all. (2019) megerősítő bizonyítékokat ad arra, hogy a szankciók bizonyossága és pontossága (időszerűsége – celerity, timeliness) növeli a válaszadók azon szándékát, hogy megfeleljenek a információbiztonsági szabályzatok változásának. A válaszadók jelenlegi gyakorlatához kapcsolódó tehetetlenség csökkenti a válaszadók megfelelési szándékát. Annak ellenére, hogy léteznek bizonyos gyors és súlyos következmények az információbiztonsági szabályzatok megsértésére, az egyének tehetetlensége akadályozni fogja, hogy viselkedésbeli szándékukat betartsák.

Az egyének viselkedését többször azonosították a szabályzat kudarcának egyik elsődleges okaként. Ahogy Leach (2003) állítja: „A rossz vagy elfogadhatatlan felhasználói viselkedés jelentős, talán a legfontosabb meghatározója a vállalat által elszenvedett biztonsági események szintjének.” Véleményem szerint is a legtöbb információbiztonsági szabályzat kudarca oda vezethető vissza, hogy nem támogatják az alkalmazottakat, akiknek követni kellene azokat. Ezért a társaságoknak foglalkozniuk kell az alkalmazottak változásokra való hajlandóságával annak érdekében, hogy biztosítsák az információbiztonság változásainak hatékonyságát. Ez a kommunikáció a szabályzat kialakításával, az abba történő felhasználói, szerepkör alapú résztvevők bevonásával kell, hogy kezdődjön.

Felmerül gyakorlati oldalról, hogyan lehetséges ezt támogatni; azaz hogyan kell segíteni munkavállalókat annak érdekében, hogy képesek legyenek jobban megfelelni az információbiztonsági szabályzatnak.

Annak érdekében, hogy megértsék a munkavállalók megfelelési magatartását, Bulgurcu et al. (2010) javasolja az információbiztonsági szabályzat betartásával kapcsolatos meglévő elméletek, például a TPB és a GDT használatát. Bulgurcu et al. (2010) szerint a szervezeteknek az információbiztonsági szabályzat betartásával kapcsolatos meglévő elméletekre kell támaszkodniuk, hogy megértsék a munkavállalók abbéli szándékait, hogy megfeleljenek a szabályzatnak. Az alkalmazottak nem szabad, hogy úgy érezzék, az információbiztonsági szabályzat a büntetés egyik formája, hanem olyan intézkedéseknek kell tekinteniük azokat, amelyek elősegítik a szervezet vagyonának védelmét, és ezáltal növelik a szervezet üzleti életét, így az adott munkavállaló foglalkoztatásához szükséges források védelmét is.

Véleményem szerint, Bulgurcu et al. (2010) elméletével egyetértve, ezeket az elméleteket figyelembe kell venni, mivel kutatásom és személyes megfigyeléseim is alátámasztják, hogy az

információbiztonsági vezetőnek proaktív lépéseket kell tenni annak érdekében, hogy az információbiztonság elfogadott, könnyen érthető és csak az adott szerepkörre (kockázatra) érvényes lényeges információkat kelljen elsajátítania, vagy legalábbis munkakörében nem releváns biztonsági elvárások elolvasása, elsajátítása ne legyen előírva. Ehhez szükséges, hogy az információbiztonsági vezető a megfelelő szerepköröket, folyamatokat, a kezelt adatok körét stb., összességében a kockázatokat azonosítsa, és szerepkör- vagy kockázatalapú legyen az információbiztonsági szabályzat és oktatás.

Áttekintve a nemzetközi szakirodalmat, az általam áttekintett szakirodalmak alapján a kutatóknál nem jelenik meg kellően markánsan annak igénye, hogy az információbiztonsági szabályzatok kidolgozási munkálataiba a felhasználók, szerepkörök bevonásra kerüljenek. Valamint nem jelenik meg kellő súllyal a szerepkör alapú kivonatok fontossága sem az információbiztonsági szabályzatokban. Fontos megjegyeznem, hogy ez nem csak a felhasználók szemszögéből fontos. A megfelelő minőségű információbiztonsági szabályzat kialakítása érdekében az információbiztonsági szakembernek vagy szakembereknek releváns képek kell kapniuk a munkaszervezet folyamatairól, az azokban kezelt adatok köréről, besorolásáról, az ezeket érintő kockázatokról stb. Az egyes munkafolyamatokat végző munkavállalók bevonása nélkül ez nem lehet teljes körű. Hiszen az információbiztonsági szakember sem ismerheti minden jelentős (értékteremtő, üzletileg fontos) területét az adott szervezetnek.

Amennyiben ilyen hiányossággal indul, akkor az információbiztonsági szabályzat sem tud teljes mértékben eleget tenni a funkciójának. Másrészről a jó és teljes szabályzat vélhetőleg elég terjedelmes, így annak elolvasására nehezen vehető rá a munkavállaló, hiszen számára csak a saját munkafolyamataihoz releváns tudás a lényeges. Így tapasztalataim szerint, még ha el is kezdi a teljes információbiztonsági szabályzat elolvasását, az első olyan oldalakkal találkozva, amelyek az adott személy munkakörében irrelevánsak, abba fogja hagyni a szabályzat megismerésére tett lépéseit, erőfeszítéseit. Ebből következik, hogy szerepkör alapú kivonatok szükségesek. Ez viszont visszavezet az első lépéshez, hogy az információbiztonsági szakembernek mélyrehatóan meg kell ismerni a szervezet folyamatait, az abban kezelt adatokat, releváns kockázatokat stb.

Rostami (2019) eredményeit feldolgozva azt találtam, hogy a szabályzatok 22%-ában van csak jelen a felhasználók bevonására való utalás (user involvment), míg a szerepkör alapú kivonatok (taylored policy) tekintetében 6%-os értéket mért. Kutatásaim során a szerepkör alapú kivonatok tekintetében én valamivel magasabb értéket mértem, a válaszadók 23%-a mondta, hogy létezik valamilyen kivonat. Tapasztalataim a szabályzatkidolgozás tekintetében hasonlóak, azaz rendkívül alacsony az egyes szerepkörök, szakterületek bevonása a szabályzatokba, valamint a

szerepkör alapú kivonatok hiánya is egyértelműen megállapítható nemcsak szakirodalmi, de gyakorlati szinten is.

Talbot és Woodward (2009) szerint az információbiztonsági szabályzat figyelemmel kísérésének és értékelésének egyik célja mérhető eredmények elérése, amelyek megmutatják a felhasználók viselkedését. Ezeket az eredményeket kell majd felhasználni a munkavállalók teljesítményének a biztonságpolitikának való megfelelés szempontjából történő felmérésére. A biztonságpolitikának való megfelelés ellenőrzése során ösztönözni és jutalmazni kell azokat a munkavállalókat, akik bizonyítják a magas szintű megfelelést a szabályzatban foglalt követelményeknek. Másrészt azokat, akikről kiderül, hogy megsértik a szervezet információbiztonsági politikáját, figyelmeztetni és szankcionálni kell. (Talbot és Woodward, 2009) Véleményem szerint ugyanakkor az információbiztonsági szempontból való jó teljesítés, példamutatás jutalmazása, ennek megszervezése kihívások elé állítja az információbiztonsági vezetőt, mivel valamilyen szinten ez költséget, erőforrás-szükségletet generál, amelyhez szükséges források fedezete kihívásokat rejthet.

Szuba (1998) azt állítja, hogy a munkavállalók bevonása az információbiztonsági politika kidolgozásába a munkavállalók elköteleződését támogatja, miközben megteremti részükről is az információbiztonsági politika tulajdonjogának érzetét. Ezzel az állítással egyetértek, bár szerintem alapvetően a kialakítás során megvalósuló kölcsönös és kétirányú kommunikáció, egyeztetés, visszacsatolás eredményezi azt, hogy az információbiztonsági vezető és az adott munkaszervezeti szerepkört betöltők egymást támogatják a jobb megértésben a kockázatok csökkentése érdekében a szabályzat létrehozása, vagy frissítése során. Az alkalmazotti támogatás tehát azon végfelhasználók támogatására vonatkozik, akik egy szervezetben különféle tevékenységet végeznek. Bizonyos számosságú halmazokba rendezhetően tipizálhatóak a szerepkörök (kockázatok).

Tudományos szakirodalmat erre vonatkozóan nem találtam, de a információbiztonsági szabályzat kidolgozása során jelentkező személyes kapcsolatoknak és szinergiáknak a kialakulása akár külön kutatásra is alkalmas lehet.

Maynard et al. (2011) pedig kifejezetten azt javasolja, hogy a végfelhasználói közösséget vonják be a fejlesztési erőfeszítés részeként annak biztosítása érdekében, hogy a szervezet multidiszciplináris jellege beépüljön az információbiztonsági politika fejlesztési folyamatába. A végfelhasználók bevonását már korai szakaszban javasolt megtenni, hogy lehetőséget biztosítsanak a hibák és nehézségek azonosítására, amelyeket ezután orvosolni lehet a biztonsági szabályzat végrehajtása előtt. „Ha a szabályzat dokumentumai nehezen érthetőek, akkor a

felhasználók nem olvassák el azokat teljesen, vagy elmulaszthatják a helyes megértésüket, és ezzel szükségtelenül kockáztathatják a biztonsági kompromittálást." Diver (2007) szerint.

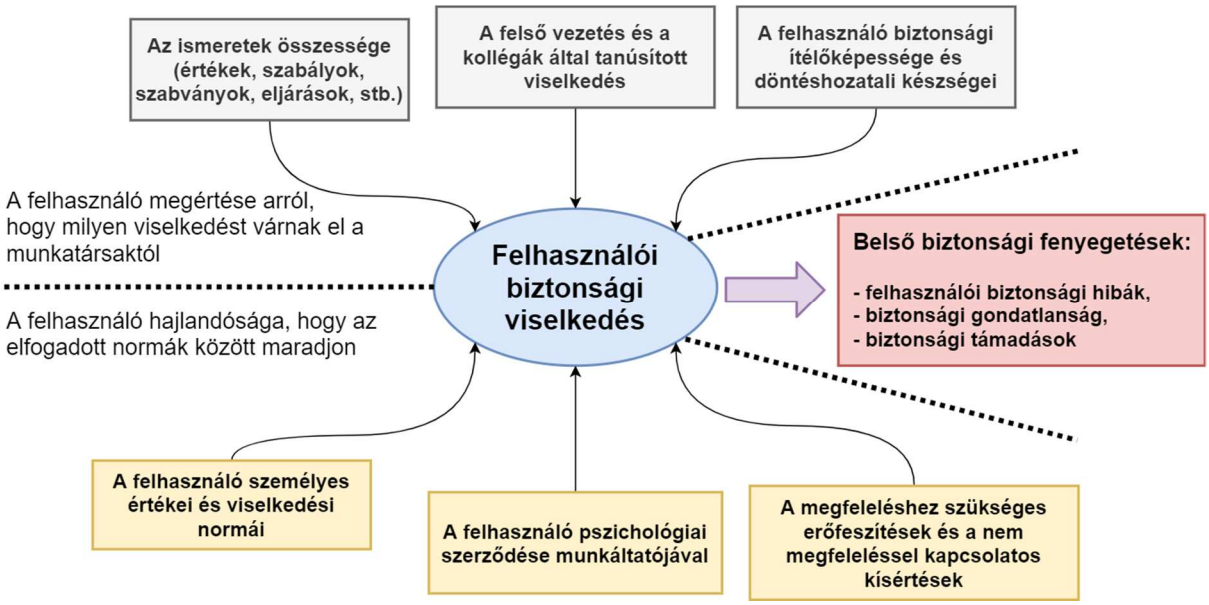
Simon (1957) a képzést a szervezeti befolyás mechanizmusának tekinti. A képzés folyamatát 1957-ben még nem részletezi, de természetesen mi már hozzáérthetünk sokféle módszert és új, modern csatornát. A szervezetek kiképzik a tagjaikat az ismeretek és készségek elsajátítása érdekében, amely lehetővé teszi a munkavállalók számára, hogy a szervezeti célokkal összhangban (megfelelő, a helyzetnek megfelelő) döntéseket hozzanak. A biztonság szempontjából a képzés témája összefonódik a tudatossággal. A szervezeti tudatosság programja gyakran egy szélesebb körű biztonsági képzési program kezdeti fázisa. A tudatosítás figyelmezteti az alkalmazottakat az információbiztonság kérdéseire. (Straub és Welke, 1998)

A képzési program meghirdetése felkészíti a felhasználókat arra, hogy hivatalos képzési program keretében megkapják az információbiztonsággal kapcsolatos szükséges alapelveket, gyakorlatokat. A biztonsági tudatosság elősegíti a képzési anyagok megerősítését ciklikus és folyamatos biztonsági emlékeztetők és események révén Hansche (2002) szerint. A képzési és tudatosítási programok felhasználhatók a szervezet kultúrájának befolyásolására Schein (1995) szerint a kedvező biztonsági gyakorlatok és gondolkodásmód előmozdításával.

A fentiekkel egyetértésben és összhangban nagyon jó megfogalmazásnak tartom a "szervezeti befolyásolás mechanizmusát", mivel ez valóban nagyon jól érzékelteti, hogyan lehetséges a munkavállalókat befolyásolni, rávenni bizonyos gyakorlatokra. Így sokkal érthetőbbek lesznek kutatásom és megfigyelésem azon megállapításai, hogy az írott szabályzat, az e-learning oktatás és a tantermi, élő oktatás ebben a sorrendben hogyan tud egyre mélyebb vagy hosszabban tartó változást, gyakorlatba épülést elérni.

Barman (2002) a tudatosságot és a képzést következetes és folyamatos tevékenységnek és folyamatnak tekinti. Világossá teszi, hogy ennek a funkciónak a fontossága kiemelkedő: „A biztonsági tudatosság képzésének és oktatásának fontosságát nem lehet eléggé hangsúlyozni. Ha a szervezet komolyan veszi az információbiztonsági politikát, és minden érdekelt felet megtanít a fenntartásában játszott szerepükről, akkor az alkalmazottak a politikát munkájuk szerves részévé fogják tenni." Whitman (2008) kijelenti: „Az információbiztonsági politika végrehajtásának rendkívüli jelentősége van abban, hogy a politikákat frissnek tartsuk a munkavállalók fejében. (…) A munkavállalók tudatosságát az egyik legnagyobb kihívásnak tekintik a biztonság általános megvalósításában." A szakirodalomban mások szélesebb körű képet állítanak fel a felhasználói viselkedésről szóló tudatosságról, amelynek képzése az általános felhasználói magatartás javításának egyik része. További tényezők befolyásolhatják a felhasználói biztonsági magatartást, ideértve a felső vezetés elkötelezettségének és a felhasználó személyes értékeinek és magatartási

normáinak érzékelését (Leach, 2003). Egyetértek azzal az állásponttal, hogy folyamatos és ciklikus tevékenység kell, hogy legyen a biztonsági-tudatossági szint fenntartása. Személyes megfigyeléseim azt is alátámasztják, ahogy disszertációmban is megfogalmazom, hogy van egyfajta lefutása az oktatások során megszerzett tudásnak – ezt a felejtési görbe kapcsán részletesebben kifejtem. Ez a jelenség számos életszerű okra vezethető vissza. Egyrészt "nem tapadt meg", nem volt kellően releváns az egyén munkafolyamataiban vagy magánéletében az oktatási téma. Vagy pedig, bár releváns (lett volna), de az elmúlt időszakban (1-3-6-12 hónap) nem történt megerősítés. Vagy releváns az incidens, így vagy feledésbe merült, vagy a gyakorlati tudásból kopott ki.



6. ábra: Biztonságtudatos viselkedést befolyásoló tényezők, a forrás saját szerkesztés (Leach 2003 alapján)

Ruighaver et al. (2007) szerint a szervezeti kultúra szignifikánsan meghatározza az alkalmazottak biztonsággal kapcsolatos attitűdjét. Schein (1996) a szervezeti kultúrát úgy definiálta, mint az alapvető feltételezéseket és hiedelmeket, (1) amelyeket a szervezeti tagok osztanak, és (2) amelyek elég jól működnek ahhoz, hogy érvényesnek lehessen őket tekinteni, és új tagoknak taníthatók legyenek. Tekintettel arra, hogy az információbiztonság általában menedzsmentprobléma, egy szervezet biztonsági kultúrája tükrözi azt, hogy a menedzsment hogyan kezeli a biztonsági problémákat. (Schein, 1996) Az irodalommal összhangban a szervezeti kultúra olyan tényező, amely befolyásolja a biztonságpolitika fejlődését, mivel a szervezet kultúrája jelentősen meghatározza az alkalmazottak biztonsággal kapcsolatos általános hozzáállását. Például, ha egy szervezet kultúrája ellenségességet vált ki a információbiztonsági szabályzattal szemben, amelyet az alkalmazottak ésszerűtlennek tartanak, a biztonsági személyzet számára nehézségekbe ütközhet az adott szabályzati elem betartatása.

A szabályzatnak elég egyértelműnek kell lennie ahhoz, hogy segítségével a munkavállalók rendkívüli körülmények között is megfeleljenek a szervezeti feltételeknek. (Fulford and Doherty, 2003)

A munkavállaló, annak eldöntésekor, hogy betartja-e a szervezet információbiztonsági szabályzatát, mérlegeli ennek költségeit vagy erőfeszítéseit, és ezek az általa észlelt válaszköltségek (perceived response cost) negatívan befolyásolhatják az információbiztonsági szabályzat betartásához történő hozzáállását (Bulgurcu et al., 2010). Ha egy alkalmazott úgy gondolja, hogy egy tevékenység elvégzéséhez vagy a szabályzat betartásához „költségek" merülnek fel, dönthet úgy, hogy nem teljesíti azt, míg válaszadási/teljesítési/megfelelési költség hiányában ezt teljesítette volna (tehát ha nem kerül erőfeszítésbe neki a teljesítés, akkor megfelel, ha ez energia-, idő- vagy egyéb befektetéssel jár, akkor nem biztos). Az emberek hajlandóak egy tevékenységet végezni mindaddig, amíg ez nem kerül számukra extra időbe, pénzbe vagy erőfeszítésbe, energiába.

A szervezet információbiztonsági szabályozása azonban nem csak kizárólag a munkavállalókra kell, hogy kiterjedjen. A szervezet szigorúan vett határain túlra, a beszállítókra és a más munkaviszonyban foglalkoztatottakra is előírásokat, elvárásokat kell definiálni. Coyle-Shapiro és Kessler (2002) úgy találta, hogy az ugyanazon szervezetben lévő ideiglenes és állandó munkavállalók eltérőek a szervezeti elkötelezettségük szintjén, mivel a tanulmány megállapította, hogy az állandó munkavállalók inkább elkötelezettek a szervezet mellett, mint az ideiglenes munkavállalók. Azt is megállapította, hogy a szervezeti elkötelezettség pozitívan befolyásolja az alkalmazottak magatartási szándékát a információbiztonsági szabályzat betartására. (Coyle-Shapiro és Kessler, 2002) A szervezeti elkötelezettség hatása a viselkedési szándékra erősebb az állandó alkalmazottakban, mint az ideiglenes alkalmazottakban. Az állandó alkalmazottak nagyobb pszichológiai beruházásokkal bírnak a szervezet iránt, és így nagyobb elkötelezettséget vállalnak a megfelelés iránt is. (Sverke et al., 2005)

Ez is megerősíti megfigyeléseimet, illetve alátámasztja kutatásom megállapításait. Egyrészt alacsonyabb elkötelezettségűek a valamilyen egyéb jogviszonyban foglalkoztatott munkavállalók. Így még jelentősebb az az igény, hogy szerepkör alapú kivonat legyen számukra is. Azaz csak a számukra releváns (legszükségesebb) információ legyen átadva, annak ismerete és betartása viszont legyen megkövetelve.

A Da Veiga (2016) által végzett empirikus tanulmány kutatási megállapításai: az általános információbiztonsági kultúra átlagértékei szignifikánsan pozitívabbak voltak azon alkalmazottak részéről, akik elolvasták az információbiztonsági politikát, mint azoknál, akik nem. Ugyanakkor fontosnak tartom megjegyezni, hogy egyfajta érdeklődés és motiváltság szükséges ahhoz, hogy

valaki egy több tucat vagy százoldalas információbiztonsági szabályzatot elolvasson. Így nem ugyanarról a motivációs szintről indul az, aki elolvasta, mint aki nem. A nagy kérdés inkább az, hogy miért olvasta el, vagy hogy milyen mélységben olvasta-el. Volt-e kivonat, és azt olvasta-e el? Mindenesetre Da Veiga (2016) a kutatási következményeket úgy határozza meg, hogy az információbiztonsági kultúrát időről időre meg kell mérni és össze kell hasonlítani a változások nyomon követése, valamint az információbiztonsági kultúra javítását célzó intézkedések azonosítása és prioritásainak meghatározása érdekében. Ha az alkalmazottak elolvassák az információbiztonsági szabályzatot, akkor ez pozitív hatással van a szervezet információbiztonsági kultúrájára. Gyakorlati javaslatként pedig Da Veiga (2016) úgy fogalmaz, hogy a szervezeteknek gondoskodniuk kell arról, hogy az alkalmazottak elolvassák az információbiztonsági politikát az emberi kockázat, a kapcsolódó hibák és események minimalizálásának elősegítése érdekében, és végül erősebb információbiztonsági kultúrát ösztönözzenek magasabb szintű megfelelési magatartással. Bár Da Veiga munkássága az információbiztonsági kutatások terén számottevő, ugyanakkor célként sokkal inkább azt érdemes megfogalmazni, hogy a munkavállalók alkalmazni tudják a munkafolyamataikban releváns információbiztonsági ismereteket, mint azt, hogy elolvassák az információbiztonsági szabályzatot.

Ugyanakkor két évvel az előbbi kutatás előtt Da Veiga és Martins (2014) megállapítja, hogy a támogatott információbiztonsági kultúra idővel pozitívabbá vált, és a javulás egyik okát a "képzési és tudatosítási kezdeményezések"-ben látja. A második lényeges megállapítása a cselekvési tervek végrehajtásával és az információbiztonsági szabályzatot elolvasó alkalmazottak számának növekedésével kapcsolatos.

Egy 2010-es kérdőíves felmérés után az információbiztonsági szabályzatra összpontosított figyelemfelkeltő program került végrehajtásra kutatásában, amely havi e-maileket tartalmazott, amelyek elmagyarázzák az információbiztonsági politika konkrét követelményeit. Összeállítottak egy brosúrát is, amely a szabályzat könnyen érthető nyelven készült összefoglalóját tartalmazza. A közleményekben hangsúlyozták a információbiztonsági szabályzat helyét és az olvasás fontosságát. Azok az alkalmazottak, akik elolvasták az információbiztonsági szabályzatot, jobban megértették azt. (Da Veiga és Martins, 2014)

Saját kutatásaim megerősítették ezen állításokat. Az érdekes, figyelemfelkeltő és érthető (nem szaknyelvi) anyagok publikációja az intranet oldalon jó látogatottsági eredményeket hozott. E-learning oktatás kapcsán és tantermi (élő) oktatás kapcsán még magasabb részvétel és visszajelzési arány volt tapasztalható. Azaz véleményem szerint ezen módokon még tovább növelhető az információbiztonsági szabályok megértése, követése.

2.1.3. A SZOROSAN KAPCSOLÓDÓ SZABVÁNYOK ÁTTEKINTÉSE

Nem hagyható el a disszertációhoz az információbiztonság miatt szorosan kötődő szabványok és „de facto” szabványok, nemzetközileg elterjedt és alkalmazott gyakorlatok áttekintő bemutatása. Az információbiztonsági oktatás kérdésköréhez szorosan kapcsolódik az információbiztonság, annak érettsége és az informatikai irányítás, annak szervezésének témaköre is. Csak a legrelevánsabb szabványokra kitérve is meg kell említeni az ISO/IEC 27000-es szabványcsaládot. A köz- és szakmai nyelvben is leginkább elterjedt az ISO/IEC 27001:2013 (vagy Magyarországon az MSZ ISO/IEC 27001:2014). Azonban a 27000-es szabványcsalád jelenleg 42, esetenként több részből álló szabványcsomaggal fedi le a területet.

Ahogy disszertációmban már említettem a tanúsító szervezetek relevanciáját az információbiztonsági területen, itt is mindenképp szükséges megemlíteni az ISACA által nyújtott *Control Objectives for Information and Related Technology* rendszert, amely az ötödik verzióban már csak COBIT néven használatos. Ez egy átfogó, nemzetközileg elfogadott keretrendszer a vállalati információ és technológia (IT) irányítására és menedzselésére, amely segíti a vállalat vezetőit és vezetőségét az üzleti és kapcsolódó IT célok megfogalmazásában és elérésben. A COBIT öt alapelvet és hét megvalósítási tényezőt ír le, amelyek segítik a vállalatokat a jó IT-hoz kapcsolódó irányítási és menedzsment gyakorlatok fejlesztésében, implementációjában, valamint folyamatos javításában és felügyeletében. (Megjegyzés: A COBIT korábbi verziói az IT folyamatokhoz kapcsolódó kontrollcélkitűzésekre, az IT folyamatok vezetésére és kontrolljaira és az IT irányítási szempontjaira fókuszáltak. A COBIT keretrendszer alkalmazását és használatát a támogató termékek egyre növekvő családja segíti elő. (Forrás: ISACA, https://isaca.org/cobit)

Az informatikai szolgáltatás irányítási rendszere (MSZ ISO/IEC 20000-1:2013 szerinti tanúsítás), a CCTA (Central Computer and Telecommunication Agency – Központi Számítástechnikai és Távközlési Ügynökség) támogatásával elindítottak egy programot, amely egységes szerkezetben próbálta meg dokumentálni a jó és sikeres gyakorlatot (best practice). Ez a dokumentációsorozat, az *IT Infrastructure Library* (ITIL), IT Infrastruktúra Könyvtár, azzal a céllal gyűjtötte össze és írta le a bevált gyakorlati tapasztalatokat, hogy azokat felhasználva a kormányzati területen javítsák az informatikai infrastruktúra működtetését. A sorozatban több mint 40 kötet látott napvilágot, és ez lett az alapja és névadója a kialakult módszertannak. Az ennek nyomán megszületett brit kormányzati ajánlás a 10 legfontosabb témakört kiválasztva hozta létre ITIL néven azt az informatikai szolgáltatásirányítási, üzemeltetési módszertant, amely azóta „de facto” nemzetközi szabvánnyá vált. (Forrás: KFKI)

ISO/IEC 20000-1:2018, Information technology — Service management — Part 1: Service management system requirements és az *ISO/IEC 20000-2:2019 Information technology — Service management — Part 2: Guidance on the application of service management systems* címmel jelentek meg és adnak útmutatást a szolgáltatásmenedzsment-rendszer (service management system, SMS) létrehozásához, megvalósításához, karbantartásához és folyamatos fejlesztéséhez. (Forrás: https://www.iso.org/)

Magyarország és a közigazgatás számára transzparensen rendelkezésre álló információs erőforrások kapcsán meg kell említeni az alábbi ajánlásokat: Az 1994-es Informatikai Tárcaközi Bizottság ajánlásai közül a 8. sz. ajánlás az *Informatikai biztonsági módszertani kézikönyv* nevet viseli. Talán ez volt az első ilyen, a teljes közigazgatás számára elérhetővé tett ajánlás. Az ajánlás a közigazgatás korszerűsítéséről szóló 1026/1992. (V.12.) Korm. határozat a közigazgatási informatika fejlesztésével összefüggő konkrét feladatokra és ehhez kapcsolódóan a központi államigazgatási szervek informatikai fejlesztéseinek koordinálásáról szóló 1039/1993. (V.21.) Korm. határozatra reagál. Már ebben az 1994. évi 8. sz. ajánlásban megjelenik az oktatás fontosságára való figyelemfelhívás: „A munkatársak beiskolázása, oktatása és információkkal való ellátása szükséges előfeltétele a biztonsági intézkedések elfogadásának."; „A biztonságtudat kialakítása és megtartása."; „Kioktatás a jogi helyzetről, az érvényes szabályozásokról."; „A képzés kiterjesztése az informatikai biztonságra is."; a kockázatoknál mint gyenge pontoknál megjelenik a „Nem kielégítő kiképzés" és a „Hiányos biztonságtudat". Ez az ajánlás tehát 1994 májusától hozzáférhető iránymutatást adott a közigazgatási döntéshozóknak.

Ezt követte az 1996-os Informatikai Tárcaközi Bizottság ajánlásai közül a 12. számú, amely az *Informatikai rendszerek biztonsági követelményei* címet viselte. A 12. számú ajánlásban megfogalmazásra került, megjelent egy oktatási életciklus is, azaz kitért az oktatásra, vizsgáztatásra, a rendszeres továbbképzésre és ezek megszervezésének felelősségére is. Azaz már sokkal részletesebb előírásokat tartalmaz az oktatásra nézve.

Ezt követően 2008-ban kiadtak egy ajánlásgyűjteményt, 25-ös számmal. Ezen ajánlások idejüket megelőzték, azonban, ahogy nevében is szerepel, szintén ajánlásként jelentek meg. Az ajánlásgyűjtemény megfogalmazza, hogy a „felhasználók tudatában legyenek az informatikai biztonság fenyegetéseinek", sőt ezen túlmenően a képzések hatékonyságának mérésére is felhívja a figyelmet: „Ahhoz, hogy a szervezet megbizonyosodjon az oktatások hatékonyságáról és hatásosságáról, utólagos ellenőrzési rendszert, folyamatot kell kialakítania." (Közigazgatási Informatikai Bizottság 25. számú Ajánlása, Magyar Informatikai Biztonsági Ajánlások – MIBA, 2008) Mindezen dokumentumok tehát a közigazgatás, a döntéshozók rendelkezésére álltak, az

oktatással kapcsolatos szerepkörökre is adtak támpontokat, sok egyéb szempontrendszer mellett az információbiztonsági irányítási rendszert, rendszertant ingyenesen tettek elérhetővé. A KIB ajánlások felsorolása a 10. számú mellékletben olvasható. Az ajánlások alkalmazásáról nem állnak rendelkezésre pontos mérések, azok nem voltak kötelező érvényűek. Feltételezhető, hogy mindenképpen jelentős, további változás, javulást volt, amikor ajánlásból kötelező érvényű dokumentum született, kiadásra került a 2013. évi L. törvény, majd a BM 41/2015. rendelet. Ezekben szintén megtalálható az oktatásra vonatkozó követelmény. Illetve mindenképpen meg kell említeni a Magyarország hálózati és információs rendszerek biztonságára vonatkozó Stratégiájáról szóló 1838/2018. (XII. 28.) Korm. határozatot. (Forrás: https://njt.hu/)

2.1.4. A SZOROSAN KAPCSOLÓDÓ MINŐSÍTŐ KÉPZÉSEK ÁTTEKINTÉSE

Disszertációs témám szempontjából az információbiztonsági tudatosság, a szabálykövetési hajlandóság növelési lehetőségét vizsgálom. Ebben nagy szerepet játszhatnak az információbiztonsági képzések, vizsgarendszerek és ajánlások, így felsorolásszerűen az alábbiakban mindenképp kitérek ezekre.

Az információbiztonságiszakember-képzés helyzetének rövid áttekintését is fontosnak éreztem, azonban szigorúan a témámhoz szükséges vonatkozásban és mértékben. Ennek egyik vonatkozása az információbiztonságiszakember-képzés Magyarországi lehetőségeinek áttekintése, valamint a minősítések, szakmai szervezetek listaszerű bemutatása.

A jelenleg hatályos szabályozás már nem csak ajánlásként, hanem kötelező elemként rögzíti, hogy a 2013. évi L. tv. hatálya alá tartozó (közigazgatási) intézmények olyan információbiztonsági szakembert foglalkoztassanak, aki az előírt végzettséggel rendelkezik, vagy az szakmai gyakorlattal került megalapozásra. Ezen kitételtől eltekintve két fő képzési irány áll rendelkezésre. Az egyik az ISACA szervezet által kiadott négyfajta (CISA, CISM, CRISC, CGEIT) minősítés megszerzése vagy a Nemzeti Közszolgálati Egyetem által indított Elektronikus információbiztonsági vezető szakirányú továbbképzési szak (EIV-képzés).
Ezeken az ISACA és NKE által indított képzéseken kívül Magyarországon továbbá az Óbudai Egyetem és a Gábor Dénes Főiskola indít információbiztonsági képzéseket. (Forrás: felvi.hu)
Ezen kívül lehetnek, vannak olyan egyetemi és főiskolai képzések, ahol egy-egy tárgy erejéig egy-egy félévben lehetőség van egy félévnyi kurzus felvételére. Tovább azt is meg kell említeni, hogy a nemzetközi ISACA-képesítések megszerzésére is szerveznek Magyarországi képzéseket.
Kitekintve a szigorúan vett 2013. évi L. tv. által definiált Magyarországi közigazgatási körből, fontos megemlíteni, hogy léteznek gyártói, szállítói minősítések is. Ez azt jelenti, hogy egy-egy nagy hardvergyártó vagy szoftverszállító kialakította a saját (termékéhez kapcsolódó) oktatási, képzési és vizsgarendszert. Példaként a teljesség igénye nélkül: Cisco Certified CyberOps Associate (CCNA), Cisco Certified Network Professional Security (CCNP), CCIE Security (CCIE), Microsoft Security Development Lifecycle, Fortinet Security Training & Certification Course és még számos gyártói minősítés létezik.

Áttekintettem a Magyarországi felsőoktatási képzési portfóliót a felvi.hu információi szerint:

- Információbiztonsági szakmérnök szakirányú továbbképzés

    - Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
- Információbiztonsági szakember szakirányú továbbképzés
    - Óbudai Egyetem Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar
- Információbiztonsági menedzser szakirányú továbbképzés
    - Jelenleg „Egyetlen intézmény sem indítja a képzést."
- Adatvédelmi és információbiztonsági menedzser szakirányú továbbképzés
    - Gábor Dénes Főiskola
- Elektronikus információbiztonsági vezető szakirányú továbbképzési szak
    - Nemzeti Közszolgálati Egyetem
- Adatbiztonsági és adatvédelmi szakjogász képzés
    - Eötvös Loránd Tudományegyetem

Ezen képzésekből Deák (2020) tíz különböző képzést azonosított, melyek az alábbi képzési típusokban érhetőek el:

- alapképzés, időtartam: 3-4 félév, BA (Bachelor of Arts), illetve BSc (Bachelor of Science),
- mesterképzés, időtartam: 2-4 félév, MA (Master of Arts), illetve MSc (Master of Sciences),
- szakirányú továbbképzés, időtartam: 2-4 félév, amely a már korábban megszerzett alap- és mesterfokozatra, főiskolai vagy egyetemi szintű végzettségre épülő oklevelet ad,

illetve fokozat és szakképzettség szerezhető.

Ezenkívül a szakmai szervezetek jelentenek még egy jelentős csoportosulást a tanúsítások és szabványok tekintetében. Ilyenek a teljesség igénye nélkül az ISACA, az EC-Council, az ISC^2 vagy éppen a NIST, míg szektor függvényében, például a gyártásközeli területen más ágazatspecifikus szakmai szervezetek, így az International Society of Automation (ISA) által létrehozott ISA Global Cybersecurity Alliance nevű szervezetet (isa.org/ISAGCA), melynek célja, hogy előmozdítsa a kiberbiztonsági felkészültséget, és a tudatosságot a gyártási és kritikus infrastrukturális létesítményekben és folyamatokban előmozdítsa.
Magyarország és az Európai Unió kapcsán is mindenképpen szükséges megemlíteni a The European Union Agency for Cybersecurity (ENISA), magyarul az Európai Uniós Kiberbiztonsági Ügynökséget.
Az ENISA-t az Európai Hálózat- és Információbiztonsági Ügynökség létrehozásáról szóló, 2004. március 10-i 460/2004/EK európai parlamenti és tanácsi rendelet alapította. Működését többször meghosszabbították, majd megbízatásának végleges meghosszabbítása a 460/2004/EK rendelet hatályon kívül helyezéséről szóló, 2013. május 21-i 526/2013/EU európai parlamenti és tanácsi

rendelettel történt. A szervezet ajánlásokat ad ki uniós szinten. Ugyanakkor ezen ajánlások figyelembe vételéről, elterjedtségéről a magyar közigazgatásban még nem készült elemzés. Ez egy későbbi kutatás tárgya lehet. A közös nyelvezet, az egységes feladat- és szerepkör-definíciók a munkavállalókat és munkáltatókat, valamint az átjárhatóságot, mobilitást és így a fejlődést is támogathatják.

Alsmadi tanulmánya például rámutat nemcsak a szakemberhiányra, hanem arra is, hogy nincs feltétlenül egységes elnevezése az egyes szakterületeknek az információbiztonságon belül. Ezen túlmenően pedig a folyamatok és rendszerek egyre összetettebbé válásával az is megfigyelhető, hogy növekszik a kiberbiztonsági szakemberek és készségek iránti igény. (Deák, 2020). A probléma feloldására egyik lehetséges megoldás a NICE Framework alkalmazása lehet. A *National Initiative for Cybersecurity Education* (NICE) *Cybersecurity Workforce Framework* az Egyesült Államok Kereskedelmi Minisztériumának Nemzeti Szabványügyi és Technológiai Intézete (NIST) által kiadott tanulmány, amely a kiberbiztonsághoz kapcsolódó munkaköröket kategorizálja. Tovább kifejti a kiberbiztonsági munkakörök tartalmát és az e munkakörök betöltéséhez szükséges képességeket, készségeket, továbbá elsajátítandó ismeretköröket. Ezáltal kiindulópontja lehet egy olyan folyamatnak, ami a keretrendszert felhasználva alapként szolgálhat a tudás, készségek, képességek meghatározására, a tantervek, tantárgyi adatlapok kidolgozására és összhangba hozására, átjárhatóbbá tételére. (Deák, 2020)

A fentiekben megfogalmazott képzések és minősítések is rámutatnak arra, hogy eltérő előképzettséggel (vagy bemeneti feltételekkel) az eltérő képzések és minősítések egységesítése könnyebbé teheti a munkaszervezést és toborzást a munkáltatói oldalon és az előrejutatást és karrierutakat a munkavállalói oldalon. Valamint arra is felhívja a figyelmet, hogy egyes képzések és minősítések között jelentős eltérések is lehetnek. Az információbiztonság oktatási szempontjából fontos didaktikai, oktatási ismeretek és tapasztalatok megléte mindenképpen javasolt, ha nem szükséges.

2.2. A KIBERTUDATOSSÁGOT (SZINTJÉT, OKTATÁSÁT) BEFOLYÁSOLÓ TÉNYEZŐK

2.2.1. INFORMÁCIÓBIZTONSÁGI TUDATOSSÁG ÉS MAGATARTÁS SORÁN ALKALMAZOTT ALAPMODELLEK

Az információbiztonsági tudatosság (security awareness) fogalmát az ISACA Glossary of terms (2015) a következőképpen határozza meg:
„Értesültnek lenni, figyelembe venni, tudatosnak és jól informáltnak lenni egy olyan szakmai tárgykörben, mely magába foglalja az adott témakör tudását és megértését és az annak megfelelő cselekvést." ("Being acquainted with, mindful of, conscious of and well informed on a specific subject, which implies knowing and understanding a subject and acting accordingly.")

A fenti definícióval kapcsolatosan Tarján (2020) az alábbiakat jegyzi meg:

- Valaminek a tudásáról és külön a megértéséről beszél, azaz különbséget tesz egy tárgykörhöz kapcsolódó betanítás (training) és a képzés (education) között, ahol
    - a betanítás alatt annyit értünk, hogy az emberek azt tanulják meg, hogy mit és hogyan kell végrehajtani,
    - a képzés pedig arra fókuszál, hogy elmondja az embereknek, hogy valamely intézkedésnek mi az értelme, és még a tennivaló egyéb kontextusát is feltárja.
- A tudatosság feltételezi, hogy a szabályokat nem csak azért követik, mert ismertek az egyének előtt, hanem azért, mert megértették, hogy miért fontos úgy cselekedni, ahogy elő van írva.

Voltaképpen a két eset különbsége, hogy szabálykövetés motivációja külső vagy belső indíttatásból fakad. Illetve, hogy az elvárás a kongruens gondolkodás része-e már. Ez is alátámasztja disszertációmban foglaltakat, hogy egyes tartalmakat hogy és milyen módon érdemes kommunikálni, milyen gyakorisággal, milyen csatornán stb. Abban az esetben, ha aktív részvételt akarunk elérni az információbiztonsági tudatossággal kapcsolatos tevékenységekben, tudatosan meg kell azt tervezni.

Lebek (2014) és szerzőtársai végeztek egy kutatást az információbiztonsági tudatosság és magatartás témakörében. Ennek keretében bár 54 használt elméletet azonosítottak, ezek közül csak négyet emeltek ki, amelyeket elsődlegesen használnak:

- Theory of Planned Behaviour (TPB) – A tervezett viselkedés elmélete
- General Deterrence Theory (GDT) – Az általános elrettentés elmélete
- Protection Motivation Theory (PMT) – A védelmi motivációs elmélet
- Technology Acceptance Model (TAM) – A technológia elfogadási modell

Azaz számos elmélet van, amely részben akár használható, indokolható az információbiztonsági tudatos viselkedés indoklására. Ez a disszertációmban is foglalt interdiszciplináris megközelítés jogosságát támasztja alá. Eszerint megfontolandó minden olyan, nem tisztán információbiztonsági, hanem oktatási, módszertani, szabályozás kialakítása, elmélet alkalmazása, amely hatékonyan képes támogatni a szabálykövetési, szabályalkalmazási hajlandóságot. Ezen fenti elméleteken kívül kiemelném a nagy népszerűségnek örvendő Social Bond Theory-t (SBT) (Hirschi, 1969), amelyet az egyén munkaszervezethez való kötődésére, annak kimutatására alkalmaznak, bár eredetileg a kriminológiában és bűnözéssel összefüggő cselekedetekre dolgozta ki. Az SBT leírja, hogy az erősebb társadalmi kapcsolatokkal rendelkező egyének kevésbé hajlamos deviáns magatartásra. Ezt az elméletet információbiztonsági szempontból alkalmazta Ifinedo (2014), aki arra ösztönöz, hogy alkalmazzuk az információbiztonság szervezeti irányelveknek és eljárásoknak való megfelelésének növelése érdekében. Deviancia akkor fordul elő, ha a társadalmi kötelék gyenge vagy megszakadt. A kötődés, a részvétel, az elkötelezettség és a személyes normák a négy fő elem ebben az elméletben. Ezek az összetevők külön-külön, de összefüggenek egymással. Minél jobban kötődik az egyén egy szervezethez, annál kevésbé valószínű, hogy eltér a szervezet politikájától, (Chapple et al., 2005) A szervezethez való ragaszkodás, a szervezeti politikák és tervek iránti elkötelezettség, az információbiztonságban való részvétel, valamint az a személyes meggyőződés, hogy a szervezeti információbiztonsági szabályzatnak való megfelelés fontos az információs eszközök megőrzéséhez, a fő tényező ebben a kutatási modellben. Safa et al. (2016) a Social Bond Theory-t használta az alkalmazottak információbiztonságának a szervezetek politikájának és eljárásainak való megfelelésére az elmúlt években. (Cheng et al., 2013)

Ezen kívül Lebek et al. (2014) az elméletek két fő típusát különbözteti meg:

- viselkedési elméletek
- tanulási elméletek

Az öt kiemelt, főbb elmélet (TPB, GDT, PMT, TAM, SBT) a viselkedési elméletek csoportjába tartozik. Ezek különféle szempontok szerint azonos kérdésre keresik a választ: Mi az oka, hogy egy alkalmazott eleget akar tenni a vállalat információbiztonsági előírásainak? Azért azt fontos kiemelni, hogy a fentebb felsorolt modellek, elméletek nem kifejezetten információbiztonságra készültek, hanem erre is alkalmazhatóak.

Parsons (2013) és szerzőtársai az információbiztonság kérdését a számítógép-használat felől közelítik meg. Ebből adódóan az ő elméletük középpontjában inkább az informatikai biztonság kérdése áll, és nem a tágabb értelemben vett információbiztonsági tudatosság.
A tanulmány az információbiztonsági tudatosság hét területére koncentrál:

- jelszómenedzsment
- elektronikus levelezés
- az internet használata
- közösségi hálózatok
- konfliktuskezelés
- mobil számítástechnika
- az információk kezelése

A felsorolásból is látszik, hogy a tanulmány az információbiztonság számítástechnikai vetületére koncentrál, és nem érinti az információbiztonság több lényeges általános kérdését. Ilyen aspektusok például:

- adminisztratív kontrollok (a jogi vonatkozások ismeretében milyen mértékű az írott szabályok és adatosztályozási elvek ismerete és követése)
- a nyomtatott média kezelése (az információ hagyományos, papír alapú megjelenése dokumentumok, termékminták stb. formájában)
- az információbiztonsági szabályokhoz való viszonyulás cégen kívüli munkavégzés esetén (home office, hivatali út stb.)
- a telephelyre látogatókhoz való viszonyulás
- az ún. „tiszta asztal” politika

A fenti lista a teljesség igénye nélkül sorol fel néhány elemet az információbiztonsági tudatosság egyéb kérdései közül. Ezzel a kitekintéssel az volt a célom, hogy rámutassak: az információbiztonság kérdése túlnő a számítástechnikai biztonság témakörén.

Illéssy, Nemeslaki, Som (2014) végzett kutatást a magyar közigazgatásban információbiztonsági szint mérésére. Majd ezt adoptálva Nemeslaki, Sasvári (2015) az információbiztonsági tudatosság gyakorlati vizsgálatát végezte el Magyarország üzleti és közszolgálati szférájában. 300 főt kérdeztek meg, és az információbiztonsági tudatosságot a következőképpen definiálták: “Egy munkavállaló általános tudása az információbiztonságról és az információbiztonsági szabályzat személyes tudomásul vétele a szervezetben.”
Az információbiztonságnak ez az értelmezése megint szűkíti a fogalmat, mert egyrészt csak alkalmazottakról beszél, habár vannak más érdekelt felek a szervezet körül (pl. ügynökök, ügyfelek, beszállítók, kölcsönzött munkavállalók, idénymunkások stb.), akiknek komoly hatása

lehet az információbiztonsági tudatosság állapotára. A „tudomásul vétel” kifejezés arra utal, hogy az egyén értelmezte és elfogadta az adott szabályozást, de inkább passzív magatartást, mintsem cselekvő hozzáállást jelent. Az információbiztonsági tudatosság jó (érett) szintje feltételez egy proaktív hozzáállást is minden érdekelt fél részéről, és emiatt a hivatkozott definíció nem felel meg az elvárásaimnak, hiszen a puszta tudomásulvételen túl a megértésen, a szabálykövetésen és annak hétköznapokban való alkalmazásán van a hangsúly.

Az Illéssy, Nemeslaki, Som (2014) által használt információbiztonsági tudatossági modell az információbiztonsági tudatosság három dimenzióját említi:

- A szervezeti dimenzió, ahol a szervezeti szokásokat és eljárásokat mérik.
- Az infrastrukturális dimenzió, melybe a szervezet környezeti és informatikai állapotát értik bele.
- Az egyéni dimenzió, ahol az általános szervezeti tudást és munkavégzési szokásokat mérik és elemzik.

A szervezeti dimenzióba tartozik az információbiztonsági tudatosság irányítási része (különösen az információbiztonsági vezető szerepére, a munkaköri leírásokra és egyéb meghatározott szerepekre fókuszálva). Az egyéni dimenzió foglalkozik a munkavállalókkal mint egyénekkel, és erősen az információbiztonsági incidensek kezelésére fókuszál. (Illéssy, Nemeslaki, Som, 2014)
Az infrastrukturális dimenzió képviseli azokat a személyeket, akik működtetik az infrastruktúrát, és biztosítják az információ áramlását, valamint az információbiztonsággal kapcsolatos tevékenységeket végzik.
Ez a háromdimenziós megközelítés megfelel a hivatkozott kutatók céljainak, de nem teljes mértékben teljesíti elvárásainkat: Ez az információbiztonsági tudatosság modell minden dimenziójában vezetőkről és munkavállalókról beszél, és emiatt ez az interpretáció is túl szűk, hiszen nem fed le minden érdekelt felet.
Maqousi et al. (2013) az információbiztonsági tudatosság kérdését folyamatorientáltan közelíti meg: „Az információbiztonsági tudatosság egy olyan folyamatos tanulási folyamat, melynek értelme van a fogadó fél számára, és mérhető hasznot hajt a szervezetnek a tartós viselkedésváltozáson keresztül.” Ez a megközelítés új dimenziókat nyit a fogalom meghatározásában:

- a tanulást folyamatként jeleníti meg,
- tehát procedurális szempontból közelíti meg a kérdést,
- középpontba állítja a tanulást és az arra való képességet,
- valamint előfeltételezi a viselkedés tartós megváltozását.

Siponen (2000) így fogalmaz az információbiztonsági tudatossággal kapcsolatban: „ez egy olyan állapot, amikor a felhasználók tisztában vannak szervezetük biztonsági küldetésével”. Így a motivációs, viselkedési elméletek, az információbiztonság tudatossági koncepciója nála is az informatikai tárgyú esetekre korlátozódik. Ezeket összegezve fontos tehát megjegyezni, hogy, az információbiztonsági tudatosság nem csak az informatikai rendszer felhasználóiról szól. A fizikai, számítógéppel nem rendelkező dolgozók is veszélyeztethetik a céget, ha rossz gyakorlatot követnek, nem rendelkeznek információval, vagy azt nem tudják a gyakorlatban alkalmazni. Valamint meg kell említeni azokat a munkaköröket is, ahol nem klasszikus számítógépen, de valamilyen információs rendszeren, gyártóegységen munkát végző, vagy ahhoz fizikai hozzáféréssel rendelkező munkakörökről van szó.
Levonva a következtetéseket ebből a széles spektrumú nemzetközi szakirodalmi áttekintésből, amely a korlátozott mértékű szakirodalmi multidiszciplinaritásra fókuszált, megállapíthatjuk, hogy nincsen egy egységesen elfogadott információbiztonsági tudatosság definíciónk, de minden egyes cikk hozzátesz valamit a fogalomhoz.

Tarján (2020) az információbiztonsági tudatosság következő fogalmát ajánlja használatra:

"Az információbiztonsági tudatosság a szervezet érdekelt feleinek tudása és attitűdje a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban."

Ennek a definíciónak van néhány nagyon fontos rétege, amelyet Tarján (2020) kiemel:

- Az információbiztonsági tudatosság az érdekelt felek széles rétegét érinti, akik mindannyian bizonyos hatással vannak a szervezet információbiztonsági tudatosságának állapotára.
- Tudás: A szabályok, eljárások és utasítások ismerete alapvető az információbiztonsági tudatosság szempontjából, de önmagában ez a fajta tudás még nem biztosít aktív védelmet.
- Attitűd: Ez pozitív hozzáállást feltételez az információbiztonsági biztonsággal kapcsolatos védelmi intézkedésekkel és kontrollokkal kapcsolatban. Azaz az emberek nem csak megértik, hogy mit kell csinálni, és az miért helyes, hanem aktívan részt vesznek a megelőző és helyesbítő intézkedésekben.
- Saját tulajdonú vagy kezelt információk: Az információ tulajdonlása fontos, de nem a szervezeti magatartást egyedüli módon befolyásoló tényező. Az adatfeldolgozás új korszaka számos esetben hoz létre olyan helyzeteket, amikor az adatfeldolgozó felelős az általa nem tulajdonolt adatokért. (Tarján, 2020)

Tehát áttekintettem a szakirodalmi definíciókat és elméleteket, és összegzésként megállapítottam, hogy az érdekelt felek gyakorlati viselkedésében, együttműködő és proaktív módon kell, hogy megjelenjen az információbiztonsági tudatosság. Így az információbiztonsági tudatosság a szervezet érdekelt feleinek tudásában, attitűdjében és viselkedésében a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban proaktív módon is meg kell, hogy jelenjen.

2.2.2. OKTATÁSI MODELLEK

Az információbiztonsági tudatosság mérése köré szorítkozva és szűkítve, csak a legszükségesebb mértékig kívánom az oktatási elméleteket áttekinteni. Ugyanakkor rendkívül fontos, hogy amikor valamilyen ismeret, tudás elsajátításáról, alkalmazási képességéről beszélünk, akkor ezeket az egyes fázisokat jól meghatározott módon fel kell tudnunk ismerni.

Ahogy dolgozatomban már bemutattam, életünk számos területén egyszerűsítéseket, általánosításokat alkalmazunk. Ez segíti és segítette a túlélést őseinknek is. Azaz nem mindenki van tisztában a maghasadás, a belső égésű motorok, elektronok áramlása vagy egyéb a hétköznapokban elterjedten használt technikák pontos hátterével, mégis használjuk ezeket.

Tudásunk jellemzően kongruens egészet alkot, azaz meggyőződésünk a megszerzett tudás, a kultúra, a csoportnyomás és egyéb információforrások összegzése. Ezeket végső soron egységes meggyőződésként, tudásként használjuk fel a hétköznapokban. Utalok itt arra, hogy az emberek ritkán tesznek meg meggyőződésük ellenére dolgokat, vagy gyakran ösztönösen, rutinból cselekszenek.

Egyik kutatásomban a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzési szakon tanulmányokat folytató (leendő) információbiztonsági vezetőknek (NKE EIV) tettem fel a kérdést minden évben arról, hogyan lehet meggyőzni valakit. Hogyan lehetséges a felhasználókat meggyőzni a szabályzatok betartásáról, vagy valamilyen szabályellenes, rossz beidegződés megfordítása érdekében? Hogyan lehetséges valakit rávenni arra, hogy költségesebb, több időt igénylő módon végezze el azt a munkafolyamatot, amit egyébként akár rövidebb idő alatt is elvégezhetne, mégha úgy akár szabályzatba is ütközne?

Mindezek miatt tehát fontos tudnunk és megértenünk, hogyan lehet hatékony információbiztonsági oktatást megvalósítani. Azaz véges számú oktatás (információközlés) alkalmával minél hamarabb az elfogadott (kongruens) tudás, sőt a használt, alkalmazott tudás részévé váljon az ismeret. A téma másik felét a tanulási görbe fejezetben (2.2.3.) elemzem. Mindezen szempontok összességében szükségesek a hatékony (költség/haszon szempontú), kockázatértékelésen alapuló információbiztonsági oktatási stratégia megtervezéséhez.

Költségként értelmezhető:

- a szabályzat létrehozása,
- a szabályzatkommunikáció,
- az oktatási anyag elkészítése,
- az oktatásra fordított munkavállalói idő, amíg a munkavállalót kiveszik az aktív munkavégzésből,
- egyéb szervezési, adminisztrációs, vizsgajavítási stb. idő,
- minden egyéb, ami cselekvést, gondolkodást, valamilyen hozzáadott energiát feltételez.

Haszonként pedig nemcsak a szabályzat ismerete, hanem a fentiekben adott definícióm is értelmezhető: az információbiztonsági tudatosság a szervezet érdekelt feleinek tudásában, attitűdjében és viselkedésében a szervezet tulajdonában vagy kezelésében lévő információs javak védelmével kapcsolatban proaktív módon is meg kell, hogy jelenjen. Amikor tanulási helyzetről beszélünk, megkülönböztethetünk nem irányított és irányított tanulási szituációkat.

Érdekes jelenség, hogy míg a csoport jobban teljesítő tagjainak hatékonyságán is inkább javított, de semmiképp sem rontott a kooperáció, addig látványos fejlődés mutatkozott a csoport azelőtt

gyengébb eredményeket hozó, vagy sokszor egy kisebbséghez tartozó tagjai esetében. (Kagan, 2001) Meg kell említeni, hogy egy klasszikus (közigazgatási) munkaszervezetben, a leggyengébb láncszem elmélete mellett sem elfogadható, hogy kiemelkedő teljesítmények (mint kiemelkedő tudatossági és tudásszint) mellett a stagnáló vagy lemaradó (nem jól teljesítő) munkavállalók rovására valósuljon meg a fejlődés. Kagan a kooperatív tanulás három fő irányát különíti el, ezek a módszerközpontú, a tananyag-specifikus, valamint az együtt-tanulási modellek. A módszerközpontú szemlélet a csoporttagok kommunikációjára, interakciójára helyezi a hangsúlyt, ennek tökéletesítése a hatékony tanulás kulcsa. A tananyag-specifikus modell azoknak a taneszközöknek és tanulási módszereknek a tökéletes kidolgozásában látja a siker kulcsát, amik a kooperatív tanulást segítik. Végül az együtt-tanulásos szemlélet olyan központi elemek megvalósulására koncentrál, mint az építő egymásrautaltság, a közvetlen interakció, az egyéni beszámoltathatóság, a társas készségek és a csoportfolyamat.

A szervezeteken belüli dolgozók által okozott fenyegetésekre összpontosítva Stanton et al. (2005) taxonómiát javasolt a biztonsággal kapcsolatos magatartás két dimenziójának besorolására: szándékosság és szakértelem szintje. Az alkalmazott magatartása szándékosan rosszindulatú, szándékosan előnyös (jótékony) vagy semleges lehet (azaz kifejezett szándék nélkül a biztonság elősegítése vagy károsítása); a viselkedés magas vagy alacsony műszaki szakértelmet is igényelhet.
A viselkedés lehet cselekvés vagy tétlenség. (Rosenblueth et al., 1943) Az aktív magatartás némi erőfeszítést igényelhet az egyéntől; az inaktív viselkedés viszont passzív, és nem igényelhet szellemi és fizikai erőfeszítéseket.
A számítógépes visszaélés a szervezeti eszközökkel való jogosulatlan, szándékos és belsőleg felismerhető visszaélést jelent az alkalmazottak részéről Kling (1980) és Straub (1990) szerint.

Ugyanakkor információbiztonsági incidenskezelés során – megfigyeléseim alapján –, ha folyamatos és konzekvens pozitív visszacsatolást alkalmazunk (“Igen, megfelelően jártál el, köszönjük a bejelentést.”), és ezt az elvárást mint kötelezettséget transzparensen kommunikáljuk, akkor csoportnormaként jön létre. Az tény, hogy gyakran nem vagy még nem a megfelelő hivatalosan kijelölt címre jelentenek a munkaszervezet egyes tagjai, de a hierarchia és felelősség növekedésével a szervezeti közép vagy felső vezetők ezen bejelentéseket már a megfelelő irányba teszik.
A szakirodalom szerint azonban nem minden csoport képes kooperatív munkát végezni.

Fontos megemlíteni, hogy megfigyeléseim szerint az awareness platformoknál alkalmazott lehetőség ezen tudományos ismeretek hiányában nem érhet el maximális hatást. Nézzük ezt meg a jobb érthetőség érdekében egy konkrét példán keresztül.

Adott egy tartalommal feltöltött (automatizálható) awareness platform. Ebben lehetséges szerepkörök vagy szervezeti egységek (vagy egyéb szempontok) szerint a tanulmányi kötelezettség előírása, kiküldése határidővel. Amennyiben az információbiztonsági vezető, képzési felelős nincs tisztában a kooperatív tanulás, az egyéni vagy csoportélmény vagy a csoportnyomás, csoportnorma jelentette lehetőségekkel, akkor azokat az erőforrásokat, ráerősítéseket nem tudja kiaknázni. Nagyon leegyszerűsítve és egyéb szempontok elhagyásával, ha egyszerre, egy időben, azaz időbeli eltolás nélkül kerül kiosztásra az oktatási anyag, akkor egyszeri kiugrás várható, mivel egyszerre, közel azonos időben, például 2 héten – 1 hónapon belül végzik el azt az iroda, munkaszervezet munkatársai. Ha viszont a munkatársak harmada kapja meg egyszerre, majd időbeli eltolással a második, majd időbeli eltolással kapja meg a harmadik harmad, akkor megvalósul a csoportélmények feldolgozása is. Azaz amikor valaki a második harmad résztvevőjeként kapja meg az előírt oktatási anyagot, ez a napi kommunikációs mozaik része lesz, így erről az első és harmadik harmadba tartozó munkavállalók is nem a hivatalos csatornán és nem szervezett módon, de értesülnek. Az első harmad számára a csoportnorma szempontjából egy megerősítés történik. A harmadik harmadra pedig prefázis révén történik meg a csoportnorma kivetítése, a nagyobb elfogadás-, befogadásra való előkészítés.

Számos gyártó kínál tartalommal előre feltöltött automatizálható platformokat információbiztonsági tudatosságok támogatására: Proofpoint, Knowbe4, Infosec, Kaspersky. (Gartner, 2019)

Ki kell még emelni az élményközpontúságot, elégedettséget, amely itt is jelentős szerepet játszik. Az oktatási platform tekintetében ez azt jelentheti, hogy a hivatalos és kötelező anyagok mellett választható anyagokat is javasolt elérhetővé tenni, azaz áldozni a szórakoztatásra is olyan módon, hogy divat, a csoportnorma elfogadott része legyen a havi nem kötelező információbiztonsági videó, hír, esemény megtekintése vagy a részvétel. Nagyobb munkaszervezet esetén megfontolandó a későbbiekben bemutatott mozaikmódszerben rejlő lehetőségek kiaknázása is. Így középtávon a csoportnorma, a szóbeszéd, a közösségi tudás részei lehetnek az információbiztonsági hírek és alapvető ismeretek.

Kutatásaim és ezek tesztelése során olyan modellt dolgoztam ki, amely a fenti jegyek mindegyikét tartalmazza, és azt tapasztaltam, hogy rövid időn belül jelentős változásokat lehet elérni az információbiztonsági szabálykövetés gyakorlatban történő alkalmazása területén, amely információbiztonsági tudatossági szint fenntartására természetesen a továbbiakban is

erőforrásokat kell szánni. Ennek lényege, hogy az érdekesség, a szemléletes „élő” bemutatás, valamint a magyarázat és a megbeszélés is megjelenik az oktatási ciklusban. Azonban nem szabad hagyni teljesen lecsengeni az érdeklődést.

A jobb érthetőség érdekében röviden bemutatom a modellem alkalmazását az egyik ilyen oktatási cél szerint megvalósuló képzés során.

Adott egy információbiztonsági probléma, amely kockázatként került azonosításra: a céges bankkártyák megfelelően biztonságos használatának kérdésköre.

Elméleti előadás, ismertetés révén felvezettük a bankkártya kérdéskörét – érthetően, de röviden, hiszen mindenki rendelkezik vele a magánéletben is, ezt a kapcsolatot erősítjük. Ezzel megtörténik a bevonás, hiszen a jelenlévőknek is van bankkártyája, érdekli őket, hogy milyen veszélyek leselkednek rájuk, hogyan tudják azokat kivédeni. Ezt követi a kockázatok felelevenítése: más is költhet a bankkártyáról, ha annak vizuális, leolvasható információit meg tudja szerezni.

A résztvevők bevonása úgy valósul meg még jobban, ha a kártya szemmel is látható elemeinek rövid bemutatása is megtörténik. Azzal a kiegészítéssel, hogy ha a CVC kód látható a kártyán, nincs eltakarva, az bizony biztonsági kockázat. Ilyenkor többen előveszik a kártyájukat, és megnézik. Ez remek alkalom arra, hogy egy önként jelentkezőtől elkérjük a kártyáját demonstrációs céllal. Teljesen az alapoktól el kell mondani, hogy mit is látunk a kártyán. Ezt követi annak bemutatása, hogyan lehetséges ezeket a kártyán szabad szemmel is látható információkat leolvasni, lefényképezni, levideózni, s hogyan lehetséges ezeket az információkat felhasználni.

Itt egyrészt elhangzott egy fontos tétel: a CVC kódot le kell takarni. Valamint a kártyán lévő, szabad szemmel leolvasható információkat is bizalmasan kell kezelni.

A demonstrációra megkapott bankkártyából (jellemzően) kiolvasható az utolsó 10 tranzakció. Azaz megvalósul a „tudományos érdekesség” bemutatása. Az átlagos bankkártya- felhasználók általában nincsenek tisztában azzal, hogy a bankkártyájuk tárolhatja az utolsó pénzügyi tranzakciókat. A demonstrációra önként jelentkezőnek bemutatásra kerül, és felszólítjuk, hogy erősítse meg, hogy az Ő utolsó fizetési tranzakció láthatóak a (csak neki) bemutatott kijelzőn. Ilyenkor, amennyiben sikeres volt a kiolvasás ezt az egyén megerősíti az előadás többi résztvevője felé.

Bemutatásra kerül, hogy mini-, mikro- vagy nagyfelbontású kamerával a nem védett, kártyáról szabad szemmel leolvasható információ (pl.: CVC kód) megszerezhető. És mindez jellemzően minden résztvevőt érint, mert nemcsak céges, de magánhasználatban is van ilyen eszköze – ez kapcsolódási pont. Ez tehát két érdekesség, lehetséges visszaélési lehetőség a bankkártyahasználat

vonatkozásában. Az egyik a kártya közelébe kerüléssel információ kinyerése. A másik a kártyán szereplő adatok vizuális leolvasása.

Az eredmény az lesz, hogy az új ismerethez kapcsolódási pontok társulnak. Az élmény személyes és élő, azaz nem „csak" történet, nem „csak" videó, hanem élő demonstráció, amibe a munkavállaló bekapcsolódhat, átélheti, megtapasztalhatja és visszakérdezhet. Így jellemzően ahhoz, hogy kongruens maradjon az ember világképe, a javasolt kontrollintézkedéseket megteszi. Ezen kívül az előadó személyessé is szakmailag hitelessé válik; tehát a további információbiztonsági ajánlások befogadására is nagyobb a hajlandóság.

Itt valóban egy új fogalom került megemlítésre, mégpedig az előadó személyes elfogadása, amelyről – tekintve, hogy ez csak az egyik lehetséges átviteli csatorna – mélyebben nem értekezem.

Előfordulhat, mint minden élő (nem felvételről történő) előadásnál, hogy az átadott bankkártya vagy az adott demonstrációs eszköz nem úgy működik, mint az tervezett vagy mint ez előző ezer esetben. Ezzel számolni kell; az idő és az egyéb körülmények függvényében az előadónak döntést kell hoznia.

Az, hogy pontosan mit és hogyan szükséges oktatni, ahogy már írtam, egy folyamatos (időszakosan frissített) kockázatelemzésnek is a függvénye. Így a közigazgatás, az adott munkaszervezet elemi érdeke, hogy az információbiztonsági fenyegetések folyamatos nyomonkövetése, elemzése megvalósuljon annak érdekében, hogy megértsük, hogyan fejlődjön, milyen területen, és a megbízhatóbb védekezés kiépítése hogyan valósítható meg. Az összes jelentés, a befolyó információ összefoglalása, a vizsgált eredményekből derül ki a támadási vektor, az új kockázatok és fenyegetések. Alapvetően látható, hogy a kibertámadások nem a technológiákat célozzák meg, vagy nem kizárólag, hanem elsődlegesen az embereket Scholl et al. (2018) szerint. Mivel dolgozatomban is az információbiztonsági oktatáshoz szükséges mértékben azonosítom a szerepköröket (stakeholder), így fel kell tenni a kérdést: miért az embert veszik célba a kiberbűnözők? Solms (2010) egyik fő megállapítása az, hogy internetes és webes rendszereket vezettek be, és ügyfelek milliói megfelelő információbiztonsági tudás nélkül kezdték el használni, illetve használják napjainkban is. (Solms, 2010) Elegendő az alap, közép és felsőoktatásban elérhető információbiztonsági képzésekre, ill. azok hiányára gondolni. Mivel a rendszerek egyre bonyolultabbak, és a feltárt sérülékenységeket (részben) a gyártók viszonylag gyorsan befoltozzák javítócsomagok kiadásával, így a javítócsomagok telepítése vagy nem telepítése ismét a humán faktorra irányítja a figyelmet. A kiberbűnözők a figyelmüket a végfelhasználókra fókuszálják, sok esetben új mottójuk alapján: „Ne próbálj betörni egy vállalat informatikai rendszerébe; nagyon nehéz lehet – célozd a naiv végfelhasználót! " (Solms, 2010)

Az gondolat, hogy a felhasználót az információbiztonság leggyengébb láncszemének tartják, megtalálható számos magyar és nemzetközi tanulmányban. A cég információbiztonsági problémáit gyakran az információbiztonsági szakterület hanyagságára, a fenyegetések semmibevételére vagy a bennfentes jogsértésekre vezetik vissza Chen et al. (2008) szerint. Vagy az információbiztonsági programok hiánya, a tudatlanság, a hanyagság, az apátia, a csínytevés és az ellenállás a hibák, visszaélések gyökere Safa et al. (2016) szerint. Herath és Rao (2009) megállapította, hogy az alkalmazottak biztonsági sértésekből fakadó büntetésének gyakorisága negatív hatással van a szabálykövető hajlandóságra. Viszont ha a biztonsági irányelvek betartásának összefüggésében az alkalmazottak úgy gondolják, hogy cselekedeteik megváltoztathatják és befolyásolhatják a szervezeti információbiztonsági átfogó célt, akkor nagyobb valószínűséggel vállalnak megfelelő magatartást. Végső soron a legtöbb technikai és beállítási hiányosság azonban mind visszavezethető valamilyen emberi (szándékos vagy nem szándékos) mulasztásra, hibára.

Hámornik, Krasznay (2017) egy speciális, az információbiztonsági szerepkörön belül is szűkebb kör, a SOC (Security Operation Center – biztonsági központ) kapcsán, tehát egy mélyen technikai témában is kiemelik a humán faktort és a csoportmunka szerepét, fontosságát. A Computer Supported Cooperative Work (CSCW) ezt a modellt alkalmazza.

Tehát voltaképpen a munkavállalók oktatása, a szervezeti és csoportnorma kialakítása, az értékes visszajelzések (incidensbejelentések) fogadásához szükséges folyamatok kialakítása alapvető szükséglete az információbiztonsági szakterületnek és az egész szervezetnek a magas költségű incidensek, leállások elkerülése érdekében. Így a szoftver- hardver komponensek, a határterületet védő, belső érzékelést támogató védelmi rendszerek beszerzése, üzemeltetése és licenszelése mellett hasonlóan jelentős költséget érdemes fordítani a rendszereket használó, „üzemeltető” személyzet kiképzésére is. Számos tanulmány úgy tekint az információs rendszert használó végfelhasználóra, mint információbiztonsági szempontból a leggyengébb láncszemre. Ez természetesen túlzott leegyszerűsítése a kérdésnek, hiszen az információs rendszereknek is derülnek ki időszakosan sérülékenységei. Bár az is tény, hogy azok sok esetben szintén visszavezethetőek emberi, pl. programozói hibákra. Abban a munkaszervezetben, ahol a munkavállalókra úgy tekintenek, mint a leggyengébb láncszemre, fontos megvizsgálni, hogy a folyamatok kialakítása megtörtént-e, a munkavállalók oktatása és az oktatás hatásfoka mérésre, kiértékelésre került-e, a bejelentések és visszajelzések kialakításra kerültek-e, és hogyan támogatja a szervezet a munkavállalókat az információbiztonsági tudás fejlesztése, szinten tartása érdekében. Ha ezek közül bármelyik hiányzik vagy nem megfelelően érthető a felhasználók által, akkor ott akár kiaknázható gyengeség, kockázat keletkezhet. Egyetlen egy e-mail, egyetlen egy

kattintás elegendő lehet a technikailag legbiztonságosabb rendszer biztonsági szintjének degradációjához. Az oktatás tehát nem csak egyirányú tudásátadás, és nem is lehet csak ennyi a célja, hanem a teljes fent leírt folyamatban szükséges gondolkodni. Fontos megemlíteni, hogy az általam kidolgozott módszertan mintegy járulékos módon képes lehet a leggyengébb láncszem, de legalábbis a lemaradók, a hiányos tudással rendelkezők azonosítására, és számukra további támogatást biztosíthat a felzárkóztatás, kockázatcsökkentés érdekében. Ugyanakkor a leggyengébb láncszem ilyen jellegű értelmezésével nem értek egyet, mivel a szervezet elemi érdeke, hogy az információbiztonsági releváns szerepkörökben dolgozókat kockázatértékelés alapján folyamatosan megfelelő, elfogadott információbiztonsági szinten tartsa; ennek érdekében mérje, tesztelje, a szükséges mértékben ezen eredményekre reagáljon. Amennyiben ez nem történik meg, akkor valóban Chent (2008) idézve belsős hanyagság esetéről van szó. Ahogy nincs minden új belépő vagy meglévő dolgozó pontosan egységes szinten IKT-ismeretekből vagy az adott számítógépes alkalmazás használati szintjét tekintve, úgy az információbiztonsági tudásszint sem egységes az eltérő élettapasztalatok és képzettségek miatt. Így ebből következik, hogy egy egységes, egyenszilárdságú információbiztonsági szint eléréséhez nem elégséges fűnyíróelv-szerűen évente egy darab, egységes képzést tartani. Mint ahogy nem lehetséges ugyanazt a hatásfokot, szabálykövetési hajlandóságot, alkalmazási képességet elérni egyetlen körlevéllel vagy élő tréninggel. Megemlítendő, hogy az átviteli közeg használatában való jártasság szintén jelentősen képes befolyásolni az átvinni kívánt tudás, információ hasznosulását. (Bujdosó, 2015)

Az embereket tehát számos kutató gyakran tekinti a leggyengébb láncszemnek (Whitman és Mattord, 2005; Boss et al., 2009; Al-Omari et al., 2012). A felhasználók nem mindig cselekszenek úgy, ahogy kell Aytes K, Terry C. (2004) szerint.

Az információbiztonság egyes álláspontok szerint az emberek problémája és nem technikai probléma. (Power és Forte, 2006) Sőt, egyesek kifejezetten úgy vélik, hogy a biztonságtudatosság jelentősebben hozzájárul az információbiztonság sikeréhez, mint a technológiai tényező. (Chen, Medlin, Shaw, 2008) Míg mások úgy fogalmaznak, hogy az emberi viselkedés hozzájárul az információbiztonság megsértéséhez. (Adams és Sasse, 1999; Besnard és Arief, 2004; Maxion és Reeder, 2005)

Wood (1995) úgy határozta meg az információbiztonsági tudatosságot, hogy tudatában van az információbiztonsági technológiai megoldásoknak. Ezzel a proaktív hozzáállást helyezi ismét előtérbe – a változó technikai és műszaki körülményekhez szükséges fejlesztenie magát a felhasználónak. Korábban az információbiztonságot inkább technikai, mint emberi kérdésnek

tekintették (von Solms, 2006; Mann, 2008). Ahogy azonban fejlődik ezen tudományterület, úgy gyűrűznek be a multidiszciplinaritásból származó további megfigyelések, kutatások eredményei.

Ugyanakkor meg kell tudni különböztetni az incidensek szempontjából is a végfelhasználókat aszerint, hogy követték-e a protokollt, valamint hogy önhibájukon kívül kerültek-e a szituációba. (Whitman and Mattord, 2005.; Boss et al., 2009)

Kutatásaim során többször feltettem a kérdést, mi az információbiztonsági oktatás igazából, mi a célja és milyen módon tehető meg. Az oktatás célja, ahogy disszertációmban bővebben is kifejtem, hogy a viselkedésben idézzünk elő tartós (pozitív irányú), tudatos magatartásnak megfelelő változást. Ennek eléréséhez ki kell emelnem azt a fontos momentumot, hogy az oktatás, az információbiztonsági tudatosság fejlesztése számos csatornán és módszerrel történhet. A dolgozatomban már említett lehetséges csatornákon (intranet, teams, képregény, kvíz stb.) kívül a megszerzett tudás éles tesztelésével, azaz olyan tesztelés által, amely végén az eredményekről visszacsatolás történik, kérdőívek, rendezvények, illetve minden olyan csatorna által, ami az információbiztonsági területre, tudásra, annak szükségességére terelheti a munkavállalók figyelmét; szóbeszéd, kommunikáció, egyeztetés tárgyát képezheti.

A már bemutatott leggyengébb láncszem elméletét újra mérlegre téve, fontos lehet megemlíteni azt, hogy az emberek nem mindig cselekszenek úgy, ahogy az kell, vagy ahogy ők maguk szeretnének vagy tervezik. (Aytes K, Terry C. 2004) Itt léphet be a disszertációmban már érintőlegesen említett hiba fogalma. Manapság újragondolják az emberek jellemzését, mivel magukban a szervezeti szabályozásokban alapvető stratégiai hiányosságok tapasztalhatók, amint azt számos jelentés és tanulmány mutatja. Scholl (2018) felmérése alapján a szervezetek mindössze 50%-a szolgáltat információbiztonsági és képzési programot az alkalmazottaknak (Verton 2002, In: Scholl 2018). Azaz a felmérés idején a szervezetek több mint fele nem képezte és nem oktatta alkalmazottait információbiztonsági területen. Az összes felmért vállalat 46%-a úgy véli, hogy kritikus hiány jellemzi őket kiberbiztonsági képességeik terén az Enterprise Strategy Group (ESG) (2016) alapján. Dolgozatomban szándékosan nem hozok kiberbűnözésből, hackertámadásból fakadó példákat, mert olyan számosságú esemény történik, hogy napi szinten lehetetlen lekövetni az incidenseket. Németországban a válaszadók csak 63% -a tesz intézkedéseket az információbiztonság tudatosítására, és ezen szervezetek 40,5%-a nem méri képzése hatékonyságát az Allianz für Cyber-Sicherheit (2015) alapján. Bár disszertációmnak nem témája, említés szintjén kitérek arra, hogy bár a 2013. évi L. törvény, ennek végrehajtási rendelete, a 41/2015 BM rendelet, illetve egyéb jogszabályok Magyarországot az információbiztonsági szempontból törvényileg jól szabályozott országok dobogós helyére emelik, azonban hazánkban sem történt meg, történik meg a tudatossági szint éves vagy időszakos koordinált kiértékelése. Ez

volt disszertációm megírásakor egyik motivációm, hogy munkámmal, az általam kidolgozott modellel és a széles spektrumú nemzetközi szakirodalom és jó gyakorlatok behozásával ez ügyben későbbi felhasználásra alkalmas, a nemzeti kibertudatossági szint emelésére, mérésére alkalmas tudást hozhatok létre, adhatok át.

A németországi (megkérdezett) vállalatok fele saját bevallása szerint sem elég felkészült a kibertámadásra. Ezenkívül a 10 vállalat közül csak négy hely rendelkezik sürgősségi / folytonossági irányítással (43%) a Digitalverbund Bitkom (9/2017) alapján. A biztonsági események 74% -át 6 hónapnál hosszabb ideig nem fedezik fel a Ponemon Institute Report (2017) alapján. (Scholl, 2018)

Belátható, hogy a technológiai megoldások önmagukban nem elegendőek az információbiztonság megőrzéséhez. Tehát a szervezetekben a menedzsment és viselkedési szempontok is egyaránt kulcsfontosságúak az információbiztonsági folyamatok és a szervezet kialakításához, az adott szervezetben való kiépítéséhez. (Singh et al., 2013)

Illetve ezt alátámasztja a kifejezetten nem a technikát, nem a műszaki sérülékenységeket kihasználó támadási forma; nyilvánvaló, hogy a social enginering (SE – nincs rá elfogadott magyar fordítás) támadásoknál csak a munkavállaló felkészítése lehet hatékony védekezési mód. (Workman, 2007)

Az emberi elemnek fontos szerepe van az információbiztonság fenntartásában a mai modern szervezetekben is, a biztonsági magatartást pedig nagymértékben befolyásolja az alkalmazók és alkalmazottak személyes kockázatfelfogása. Ezek a felfogások azonban megváltoztathatók a figyelemfelkeltés és az információbiztonsági képzések segítségével. (Beyer et al., 2016) Ezért az intézmény vezetésének feladatai és kötelességei fontos szerepet játszanak (BSI, 2008). A social enginering jellegű támadások növekvő volumenére mutatnak rá kutatók. (Bányász, 2019) Fontos kiemelni azonban, hogy az egyes támadástípusok gyakran összemosódnak pont a technológia bonyolultsága miatt. Bányász (2019) megfogalmazása szerint "A social engineering egy olyan támadásforma, amely során a támadó először a kihasználható emberi tulajdonságokkal él vissza, hogy ily módon férjen hozzá megtévesztéssel, zsarolással a védett információkhoz, illetve rendszerekhez." Ezzel a definícióval részben egyetértek – talán annyiban tartom érdemesnek a pontosítást, hogy a támadó az emberi bizalommal, hiszékenységgel él vissza, és időben nemcsak az egyszeri, hanem akár a hetekig, hónapokig, azaz hosszabb ideig tartó becserkészés is ide sorolható.

A képzés hatékony módszer lehet a biztonságosabb technológiákhoz vezető biztonsági eszközök elfogadásának ösztönzésére Nottingham (2013) szerint. Azaz a vezetői szint, felső vezetők (menedzsment) oktatása, felkészítése hozzájárulhat a későbbi technikai eszközökre szánt források

jóváhagyásához is, mintegy önmagát erősítő spirál lehet, amelyet szintén az oktatás segítségével lehet elindítani és fenntartani.

Kovács (2018) így fogalmaz: “Az oktatásnak ki kell térnie arra is, hogy melyek azok az áruló, a mindennapi élet különböző folyamataihoz nagyban hasonló, attól csak kis mértékben eltérő jellemzők, amelyek alapján ha nem is lehet felismerni a támadást vagy annak szándékát, de mindenesetre az erre irányuló gyanúnak fel kell ébrednie... “

Majd kiemeli, hogy az oktatás természetesen szabályozási kérdés is, mivel annak szerepelnie kell a szabályzatban, az éves oktatási tervben. Továbbá rendelkezésre kell, hogy álljon

5. ábra: Információbiztonsági oktatási ciklus, (OPDCA) forrás: saját szerkesztés,

incidenskezelési terv, számos szabályozási területhez is kapcsolódó dokumentum. Majd így folytatja: “...nyilvánvaló, hogy a felhasználókat ezzel a tervvel csak a számukra szükséges szintig és mértékig kell megismertetni.” Hangsúlyozza, hogy optimális esetben tréning szükséges, hiszen a csak írott vagy csak elmondott ismeretanyagnak a legjobb, ha a gyakorlati szabályalkalmazási képességbe tud beépülni: “A képzésnek sok esetben tréning, azaz gyakorlás része is kell, hogy legyen, hiszen így lehet egyrészt meggyőződni arról, hogy valóban a gyakorlatban is képes a felhasználó alkalmazni az elméletben megszerzett tudást, másrészt az incidenskezelési terv próbája is egy ilyen – ellenőrzött keretek között történő – gyakorlati próba.”

A fentebbi kijelentés, hogy elsősorban az embereket és nem a technológiát támadják, talán annyiban szorul pontosításra, hogy a nagyobb gyártók a tudomásukra jutott sérülékenységeket rövid időn belül megfelelő csatornákon a javításokkal együtt jelzik. Azaz ez a process, észlelés, javítás, kompenzációs kontroll stb. alapvetően működik, bejáratott. Hogyan működhet ez abban az esetben, ha a felhasználó a célpont? Nos, ez már munkaszervezetenként eltérő: Egyrészt a

tudatossági oktatások eredményeképpen azok gyakorlatba való átültetési képessége határozza meg hogyan, milyen mértékben és milyen sebességgel képes a felhasználó jelenteni; az adott szervezeti egység, aki ezt fogadja, milyen sebességgel tudja jelentést feldolgozni stb.. Másrészt, hogy a szervezeten belüli folyamat mennyire költséges, mennyire bejáratott, ismert, és kezelése könnyű-e a felhasználóknak.

Ezért részben a biztonsági szakértőknek sem szabad a „szervezeti-tudásbeli" gyengeségeket az áldozat hibájának tekinteniük, hanem áldozatként vagy fontos tanúként kell kezelniük azon felhasználókat, akik hozzájárulnak a fehérgalléros bűncselekmények kivizsgálásához. (Ugyanakkor természetesen a tudásbeli hiányosság, gyakorlatbeli hanyagság stb. nem mentesít teljes mértékben a felelősség alól. Például a felhasználó jelentett-e, milyen gyorsan, az előírt módon tette-e? Ilyen hozzáállás azonban sok szervezetben nem található meg, és ahol ez hiányzik, a vállalatok ritkán férnek hozzá teljes mértékben az értékes visszajelzésekhez, amelyeket kaphatnának Haucke A., Pokoyski D. (2018) szerint.

2.2.3. A TANULÁSI GÖRBE, AZAZ A TUDÁS SZINTEN TARTÁSA

A tanulási görbével a szakirodalom több eltérő megközelítésben foglalkozik. Disszertációmban ebből az alábbi megfontolások relevánsnak az információbiztonsági oktatások, illetve az így megszerzett tudás gyakorlatba való átültetése, valamint ezen ismeretek „észben tartása", felszínen tartása érdekében (Gruning, 2009):

- a megszerzett új ismeretek kapcsolódhassanak a meglévő tudáshoz vagy hiedelemvilághoz, amennyiben nem, úgy az szegregált, a működő rutinnak nem lesz része
- a megszerzett tudás folyamatos szinten tartása, gondozása szükséges, mivel a (élő tudáshoz tartozó) kapcsolat megerősítés nélkül megkopik, elhomályosul, vagy a napi döntéshozatali mechanizmusban kisebb súllyal esik latba
- milyen gyakorisággal szükséges az ismétlés az információbiztonsági tudatossági szint megfelelő szinten tartásához, valamely csatornán, emlékeztető impulzust közvetíteni, legyen az egy egyszerű kommunikáció, informális vagy formális oktatás.

Egyes elméletek ezt a "felejtési görbe" megközelítésben vizsgálják, de erre értekezésemben nem térek ki.

Az információbiztonsági tudás a tudatos viselkedés szempontjából

Egy felsoroláson keresztül megvilágítva minden olyan esemény ide kapcsolható, amely abban segít, hogy az információbiztonsági elvárások a működő aktív tudáshoz tudjanak kapcsolódni, rögzülni. Mint látni fogjuk, ennek nem kell szükségszerűen formális oktatásnak lennie, hiszen hétköznapi tudásunkat sem kizárólag formális (tantermi) körülmények között sajátítjuk el.

Így ezen tipikus kommunikációs formák közé sorolható például:

- tantermi oktatás,

- e-mailes hírlevél,
- intranethír, videó, képregény,
- e-learning oktatás,
- vizsga, vizsgahatáridő-emlékeztető,
- szabadon választható rövidhír, videó
- kérdésfeltevés, kvíz, szavazás,
- egyéb program, szóróanyag, verseny,
- egyéb

Azaz valamely emlékeztető, valamilyen kapcsolódási pont létrehozására ezek bármelyike alkalmas lehet, természetesen eltérő súlyozással. Egyértelmű, hogy az intranethírekkel lehet, hogy nem érhető el olyan megértés, kötődés és olyan időtávú rögzülés, mint mondjuk tantermi oktatással. Érdemes tehát a legoptimálisabb hatás érdekében időszakosan valamilyen módon felidézni, felidéztetni a kollégákkal az információbiztonság fontosságát. Erre pedig hatékony lehet bármilyen olyan impulzus, amely azt beemeli a napi beszédtémák közé, ad absurdum a pletyka, a napi párbeszéd révén képes a felejtés ellen hatni.

Fontosnak tartom megemlíteni, hogy a legtöbb információbiztonsági képzésnél, azt megelőzően nem történik meg a kezdeti (alap) képességek meghatározása, felmérése. Optimális esetben ennek a felmérésnek úgy lenne szükséges megtörténnie, hogy legyen lehetőség azt elemezni, és eredményeit az oktatásba beépíteni. Mivel a közös szókincs, a gondolati keretek meghatározása, egységes szintre hozása nélkül soha nem is lehetséges olyan minőségű eredmények elérése. Röviden most csak javaslatként annyit fogalmazok meg, hogy az IKT- és egyéb alapvető IT- és információbiztonsági ismeretek elérése és a támogatás (a visszakérdezés lehetőségének) megteremtése kulcsfontosságú. Ez kultúraformáló jelentőséggel bír, mivel a kérdések és visszakérdezések rövid időn belül lecsengenek. Azaz, ha az adott személy az őt érdeklő adott téma kapcsán felmerült kérdésére nem kap rövid időn belül választ, akkor az adott tudás megértése, beépülése, rögzülése szenvedhet csorbát.

A szerepkörre szabott vagy kockázati felmérés során azonosított oktatási téma, adott feladatkörre előírt ismeretanyag elsajátításának, betartásának eredményessége tehát egy életciklust határoz meg.

- Az azonosított szerepkör és cél, amelyre kockázati vagy más alapon priorizálva a meghatározott tudásanyag kiírásra kerül.

- Előzetes felmérés arról, hogy az adott csoportnak milyen szinten áll jelenleg a információbiztonsági tudatossági szintje általános és specifikus területen. (Ugyanezt IKT-területen is érdemes lemérni vagy legalább mintát venni).
- Az oktatás és a hozzá kapcsolódó vizsga kidolgozása.
- Meghatározott idő után a beépülés visszamérése teszt vagy kérdőív vagy egyéb formában; annak kiderítése, hogy a megszerzett tudást képes-e a csoport a gyakorlatban is alkalmazni, és a szervezeti elvárásoknak megfelelően alkalmazza-e.
- Eredmények visszacsatolása, az oktatási ciklus folytatása.

Ez az életciklus tehát időbeliséget is meg kell, hogy határozzon, és szerepkör, vagyis kockázati besorolás szerint is szükséges differenciálni.

Ha az információkat több érzékszervvel fogjuk fel, egyszerre több helyen kerülnek tárolásra az agyban. Ezáltal könnyebben megy a felidézés. A hosszú távú memóriába való beépüléshez az első oktatást követő heti, havi és féléves ismétlés szükséges, azaz mindez a klasszikus évi egyszeri oktatások ellen szól. (Azaz több szempontból is káros vagy nem elégséges az évenkénti egyszeri oktatás.) Az első havi ismétlést követően pedig az ismeret immár a hosszú távú memóriában rögzült, és csak alkalomszerű frissítésre van szükség. Ezért ajánlatos az információkat minden hat hónapban még egyszer átnézni. Ami tehát megállapítható, hogy nem elegendő évente egyszer információbiztonsági oktatást vagy bármilyen egyéb impulzust adni a témában. A pontos eredmények és az optimális hatás érdekében javasolt felmérni, hogy az elvárt viselkedésminta, a követendő gyakorlat hogyan és milyen mélységben épült be a hétköznapokba. A tudás, illetve a gyakorlatba épülés hatékonyságának mérésére is számos lehetőség van. Ezen módokat a szerepkör, az időbeli sík, a kockázati besorolás kell, hogy meghatározza. Ide sorolhatók a példa kedvéért a kérdőívek, az információbiztonsági hírlevelek, a hírek olvasottsági statisztikái vagy a phishing tesztek kiértékeléséből származó adatok is.

Mindazonáltal szilárd meggyőződésem, hogy az elérendő cél a tanulás értelmes formája, legyen szó akár iskolai, akár munkaszervezeti tanulásról. Az értelmes tanulás eredményes, eredményességének mutatója pedig az, hogy mennyire megalapozott, a meglévő ismeretekhez igazodó, és a feladatvégzés során milyen mértékben alkalmazható a tanulás által szerzett, a legáltalánosabb értelemben vett tudás. Kérdés tehát, hogy hogyan jelenik meg a napi feladatvégzés, a munka folyamata során gyakorlati szinten az elméletben átadott elvárások, tanácsok, módszerek rendszere. (Ha például szeretnénk elérni, hogy a munkatársak minden incidensről referáljanak, vagy ügyeljenek jelszavaik biztonságára, akkor érdemes az ezzel kapcsolatos oktatás előtt és után is mérést végezni a kollégák eljárásaival kapcsolatban az említett

kérdésekben. Ha az eredményesség egyik mutatójának tekintjük, felmérhetjük azt is, hogy a fent nevezett tudást mennyi idő- és energiabefektetéssel sajátítják el az érintettek.) Elengedhetetlenek olyan (a gazdasági folyamatok területén is a hatékonyságot növelő) módszerek és gyakorlatok, amelyek fokozzák ennek a tanulási folyamatnak a hatékonyságát, mert az így szerzett tudás adaptívabb, strukturáltabb, használhatóbb lesz. (Hatékony tanulás, Gaskó Krisztina, Hajdú Erzsébet, Kálmán Orsolya, Lukács István, Nahalka István, Petriné Feyér Judit, 2006)

Disszertációm nem érinti a téma pszichológiai vonatkozásait, de megjegyzésként annyit hozzáfűznék, hogy a tanulás, valamint a tanultak emlékezetben való rögzülésének hatékonysága az ismereteink között létrehozott értelmes kapcsolódási pontok függvénye – ahogy azt Gaskó 1. tétele kimondja. Az ehhez kapcsolódó 2. tétel szerint előzetes tudásunk, illetve ismereteink hatással vannak a tanulás eredményességére, hatékonyságára. Gaskó tétele az emlékezet működése által nyer igazolást (l. fent), azaz a feedbackek (visszacsatolások) információfeldolgozásban játszott szerepe révén. A 3. tételben kirajzolódik a tanulás konstruktivista megközelítése – összhangban az előző két tételben leírtakkal. A konstruktivista megközelítés szerint a tanulási folyamat előzetes tudásunkra épül, és a tanulásról alkotott prekoncepcióink is befolyásolják azt – ahogy ezt az 1. és 2. tétel is kimondja.

Azaz az információbiztonsági szakterületnek még az oktatás megtervezése (és természetesen lebonyolítása, sőt, az azt megelőző mérés) előtt információja kell, hogy legyen:

- a kockázatokról, (adott terület, adott munkakör vonatkozásában azonosított kockázatok)
- a kockázatokra szánt kontrollokról (a kockázatok priorizálása, illetve a kiválasztottakra hogyan lehetséges reagálni)
- az általános információbiztonsági szintről
- mindezek alapján azonosított fejlesztési területekről

A már meglévő tudáshoz könnyebb az új információ illesztése, főleg, ha ez a tudás nem kizárólag formális (vagy tantermi) oktatásból származik. Így voltaképpen azt mondhatjuk, hogy a hétköznapi vagy a munkahelyi relevanciájú meglévő tudásunkhoz könnyebb új tudást illeszteni. Ha pedig ez érdekes módon van tálalva, vagy több érzékszervre hat egyszerre, akkor akár motivációról is beszélhetünk, amely arra irányul, hogy az átvinni kívánt információt megismerje az érintett személy.

A tanulási motiváció négy egymásra ható motivációs faktor segítségével írható le:

- kíváncsiság, érdeklődés
- a siker elérésére való törekvés, a kudarc elkerülésére való igyekezet
- a szociális elismerés igénye

- a megtanulandó anyag hasznosságának, értékének egyéni elismerése
  (Dr. Dinyáné Szabó Mariann, 2011)

Durkheim (1961, in Csányi) három szervező elvet határozott meg a motivált csoportok létrehozása és működése kapcsán: a közös akciókat, a közös moralitást és a saját érdek háttérbe szorítását, valamint leírta a transzformáció jelenségét, az új entitás kialakulását.
Disszertációm célját figyelembe véve kiemelem a csoportkialakulás utolsó evolúciós szakaszát. Ezen szakasz folyamatainak értelmezésekor fontos látni, hogy az ideaevolúció elindulása a kezdeti csoportszerkezetek sikerességének, a csoportszámok megnövekedésének, valamint az egyezkedési kultúrák létrejöttének függvénye. Összetett és összehangolt ideastruktúrák jönnek létre azáltal, hogy kisebb, elszigetelt csoportokban több generáción át öröklődnek a gondolatok, a cselekvések és az érzelmek idegi prezentációi. Egy-egy ideastruktúra olyan elemek komplex rendszere, amelyek elengedhetetlenek az idea sikeres alkalmazásához. Éppen ezért a különféle technológiák, illetve hiedelmek rendszere sok esetben kipróbált és bevált elemekre bontható le. A kisebb csoportok érintkezés általi asszimilációja révén idővel hatalmas evolúciós tér alakult ki, ez lehetővé tette különféle ideák, koncepciók korlátlan rekombinálódását, illetve új ideák születését anélkül, hogy ezek átmentek volna a kipróbálás szelekciós szakaszán. Míg eddig a csoportot alkotó egyén ideáit, életvitelére vonatkozó szabályait a csoport határozta meg, és a csoport tovább örökítette a problémák megoldására leghatékonyabbnak tartott szabályait, az egyén most választási lehetőség előtt állt. Meg kellett vizsgálnia más kultúrák és csoportok életvitelét, szabály- és hagyományrendszerét, majd felmérnie, melyik szolgál javára – s mindezt a biológiai evolúció kísérő folyamata nélkül, a választásra való felkészülés hiányában.
Ezeket a döntéseket minden egyén a saját, legjobb belátása szerint hozza meg, meglévő ismeretei, előképzettsége, a körülötte lévő csoporttól szerzett ismeretek alapján. (Csányi, 2000)
Megemlítem még Zeigarnik (1927) hipotézisét az emlékképződésről, amelynek eredményeit az 1927-es *On Finished and Unfinished Tasks* (Befejezett és befejezetlen feladatok) című tanulmányban publikálta. Ennek számomra érdekes momentuma a memóriaműködésről szóló elmélete kapcsán, hogy az aktív információgyűjtés elősegíti annak megőrzését, de az elő nem hívott információt valószínűleg könnyebben elfelejtjük. Mindezeket összefoglalva a tanulási és felejtési görbe, a nem ismételt, nem megfelelő időnként ismételt (az agy számára értéktelennek tűnő) tudás annak elhalványulásához vezethet. Ugyanakkor a információbiztonsági képzés, ismétlés, az időbeli támadások sajnos nem feltétlenül alkalmazkodnak ehhez, így szervezetten szükséges a megfelelő időben és pontokon beavatkozni; a tudást frissíteni, fenntartani szükséges. Azaz, ha adott kockázatra reagálva megtörtént a felmérés (alap tudásszint felmérése), erre

reagálva megtörtént a képzés, akkor ezen tudás előhívását valamilyen, a fentiekben részletezett csatornánk egyikén adott impulzus, emlékeztető segítségével támogatni szükséges. Ez lehet egy szimuláció vagy ismétlő oktatás, de egyéb előhívó módszer is.

Shuhaili (2014) számos tudatossági szintet eredményesen befolyásolni képes metódust említ. Az információbiztonsági tudatosság mechanizmusainak osztályozását az alábbiak szerint csoportosítja, melyeket példákkal egészítettem ki:

Olvasható anyagok lehetnek különböző kiadványok, poszterek, szabályzatok, intranetoldalak, kézikönyvek és leírások, előírások, hírlevelek, asztalra vagy másra elhelyezhető riasztások, figyelemfelhívó kiadványok, emlékeztetők és terjesztési anyagok, szervezeti szintű e-mail-üzenetek, feliratkozási lehetőségek.

Rendezvény- vagy eseményalapú lehet például az információbiztonsági nap, „brown bag seminars" – "barna táska szemináriumok".[1]

Videoalapúak, így például a webalapú foglalkozás – webinar, konferencia, számítógépes képzés (CBT), videojáték, kioszk vagy megállító LCD-tábla jellegűek, webes vagy egyéb játékok.

Figyelemfelkeltő eszközök üzenetei (Messages of awareness tools – Csecsebecsék) úgy, mint tollak, ceruzák, kulcstartók, post-it-jegyzetek, jegyzettömbök, elsősegély-készletek, tisztítókészletek, hajlékony lemezek (manapság inkább pendrive), könyvjelzők, frizbi, óra, kártya, naptár, kabalák, matricák, bögrék, poháralátétek.

Service vagy help desk (Hotline), ahol üzenetek helyezhetőek el, tipikusan telefonközpont-beköszönő szövegek.

Házirend alapú eljárások, azaz figyelmeztetések küldése, ha sérti a szervezetek politikáját, valamely szabályrendszert; kis díjakat vagy jutalmakat lehet osztani, elnyerni. Alkalmazáson belüli badge-ek, kitűzők elnyerése vagy adása. Vagy alkalmazáson belüli képek, feliratok időszakos, kampányszerű cseréje.

A felső vezetés támogatása körébe pedig az információbiztonsági csapatot sorolja a szerző.

Az oktatás során tehát azokra az elemekre kell helyezni a hangsúlyt, amelyeket a napi rutin során közvetlenül használni tudnak majd a képzésben résztvevők. Ebben kitüntetett szerepe van a folyamatok, eljárások, szabványok, ajánlások ismeretének. Egy megkérdezettünk tapasztalata az, hogy megtörtént incidensek esettanulmány-alapú feldolgozásával mind a szabályok, mind pedig az eljárások, folyamatok sokkal könnyebben átadhatók:

[1] Brown bag seminars: Ezek Magyarországon nem annyira elterjedtek még, de jellemzően a nevük is onnan ered, hogy az ebédet barna zacskóban hozó, ebéd körüli, közös ebéd közben végzett oktatásra, eszmecserére utalnak. Lehetnek díjátadó programok, személyes képzések, indukciós tréning, (ön)ellenőrzési folyamatok, tesztek és vetélkedők, keresztrejtvények, életszerű, való életből vett demonstrációk, bemutatók.

„Erre kíváncsiak az emberek. Nem elég elmondani a szabályzatot, az esetre fog emlékezni, nem a szabályzatra, illetve az eseten keresztül a szabályzatra, az elkerülhető hibákra és a helyes megoldásokra.” (Illéssy, Nemeslaki, Som, 2014)

Véleményem szerint a szabályzat vagy a jó gyakorlat ismertetése helyett egy történet elmesélése, elmondása és a konzekvenciák közös levonása sokkal hatékonyabb megértést, memorizálást, beépülést eredményezhet. Szász és Kiss (2018) kutatása is alátámasztja, hogy az adott kurzus kialakítása hatással volt a hallgatók szokásaira, megváltoztatta azok attitűdjét és mindennapi információbiztonsági tudatosságát. Salmon, K. (2010) vizsgálja a történetmesélés nyújtotta narratív lehetőségeket, és megállapítja, hogy az elbeszélések a komplex és sokdimenziós ötletek bemutatásának és közvetítésének hatékony módjai lehetnek. A jól megtervezett és jól elmondott történetek közvetíthetik az információkat és az érzelmeket, kifejezetten és hallgatólagosan, valamint a lényeget és a kontextust. A narratív menedzsment készsége, a pozitív elemek fenntartása és fejlesztése, helyes és időben történő átültetése azok számára, akiknek szüksége van rá, semlegesíti a negatív elemeket, és időnként létrehoz egy újat. Ez a modern mesemondás, az elbeszélés képességeinek használata, az elbeszélés művészete olyan területeken is utat tör magának, mint például az információbiztonsági oktatás. Ezt eredetileg nem tekintették szűk alkalmazási területnek, legalábbis eddig. Rámutatva az elbeszélés univerzumára és csábító jellegére, valamint szélesebb körű alkalmazásának szükségességére olyan területeken, mint az információbiztonság jó példa a Nemzeti Közszolgálati Egyetem által készített *Egy hacker élete* filmsorozat is.

Így fontos megemlítenem, hogy hatékony eszköz lehet az információbiztonsági oktatások során a storytelling módszere, amelyet gyakorlatban is alkalmaztam kutatásaim során, kimagasló eredményeket elérve. Salmon (2010) szerint a storytelling alaptézise azt mondja: “Mindig mesélj egy történetet!” Miért? Gondolkodásmódunk hozzászokott az elbeszélés szerveződéséhez, a fogalmi működéshez képek segítségével, amelyek egy bizonyos tapasztalati modellbe vagy mintába próbálnak felsorakozni. Ezért grafikákban és képekben élünk, képekkel és elképzelésekkel, amelyeket narratívan dolgozunk fel azzal, hogy értelmet adunk nekik, úgy alakítjuk őket, hogy beilleszkedjenek az elvárások horizontjába, megalkotva saját világunkat.

Az emberi informális kommunikáció jelentős részét, egyesek szerint kétharmadát, jelen nem lévő, más személyekről folytatott értékelő tartalmú beszélgetés teszi ki. (Dunbar, 1996; Foster, 2004). Az ilyen beszélgetéseket, amelyekben legalább egy értékelő és egy hallgató vesz részt, tekintjük pletykának. (Kurland–Pelled, 2000); Ellwardt, 2011) Jó pletykát hallani és pletykálni mindenki szeret, mégis magához a pletykához a köznapi értelemben pejoratív konnotációkat fűzünk, elítéljük azt. Miért létezik akkor, és miért olyan elterjedt a pletyka? Miért használunk ki szinte

minden alkalmat mások háta mögött történő kibeszélésére? Ezeknek a kérdéseknek a megválaszolásához elengedhetetlen elsőként annak igazolása, hogy tényleg ilyen léptéket ölt-e az emberi társas kommunikációban a pletyka. Az említett kutatás kiinduló hipotézise az volt, hogy a pletykának pozitív közösségi funkciója van. A pletyka egy olcsó eszköz, amely biztosítja a közösség szereplőinek a reputációs kontrollját, értesít azok esetleges normaszegéseiről, és így hozzájárul a társas normák fenntartásához, a közösségi rendhez, és elősegíti az együttműködést. Felmerül számos kérdés, mely véleményem szerint az információbiztonsági norma szempontjából is igen fontos. Befolyásolja-e a pletyka a hallgató viszonyulását az adott témához? Például az érintett személy megítélésekor a hallottakkal összhangban formál-e véleményt? Kapcsolódik-e a pletyka valamely norma megszegéséhez? Hozzárendeli-e a pletykát a hallgató valamely érvényben lévő közösségi normához? Kivált-e tartózkodást a hallgatóban, ha negatív pletykával illetnek egy adott személyt? Mennyiben befolyásolja a pletyka az adott személlyel való együttműködését?

Mindezek az információtovábbításra használható nemformális, informális csatornák is felhasználhatóak az információbiztonsági szint fenntartásához.

Az informális kommunikáció formái természetes úton fejlődnek ki egy szervezetben (l. informális kommunikáció, Dobák és Antal, 2010). A grapevine (szőlőtőke), azaz az informális kommunikációs háló különféle közvetlen és véletlenszerűen létrejött kapcsolatra épül, és a szervezet egészét lefedi. Megfigyelhető, hogy működése rendszerint gyorsabb és megbízhatóbb, mint a formális kommunikáció útjai. Jól példázza ezt az a valós eset, amikor egy vezetői értekezleten hozott, leépítésekről szóló, még nem publikus döntésről néhány pillanat múlva a cég vidéki irodáiban is értesültek a titkárnői kapcsolatokon és a belső levelező hálózaton keresztül. A szerzők azonban hangsúlyozzák, hogy nem elvetendő ez a sajátos módon működő információs háló, mivel kiépülésének hátterében alapvető szükségleteink állnak; így az információ áramlása gyakorlatilag kiküszöbölhetetlen. Ez nem azt jelenti, hogy jótékonynak kell tekinteni a szervezeten belül felmerülő szóbeszédet, esetleg rémhíreket, amelyek javarészt konfliktusokkal, előmenetellel vagy éppen leépítéssel kapcsolatosak. Azonban a felmérések érdekes módon azt igazolják, hogy az informális kommunikáció jelentős részben üzleti vonatkozású, illetve közvetlenül a munka jobb elvégzéséhez kapcsolódik, így célszerű bátorítani, támogatni. Példaként említem, hogy a nem szándékos információbiztonsági visszaélésekre adott gyenge súlyú válasz, egyszerű e-mailes figyelmeztetés jó eséllyel a munkavállaló környezetében is információbiztonsági tudatossági növekedést, jobb normakövetést eredményezhet.

Azaz a megfelelő módszerek által, amely akár a szervezett storytelling előadásoktól, a tudatosan szervezett vagy tudatosan irányított informális pletykaátadásig is terjedhet, előnyt, a

meghatározott cél elérését vagy annak támogatását is el lehet várni. A jó vezető megtalálja annak módját, hogy miképpen használja fel céljainak elérésére ezt a „hálózatot". Egyrészt olyan információkhoz juthat a segítségével, amelyekhez egyébként nem nagyon van hozzáférési lehetősége; másfelől pedig ő maga is eljuttathat olyan üzeneteket, amelyek a formális csatornákon keresztül csak körülményesen adhatók át. Továbbá arra is lehetőséget kap, hogy informális kiszivárogtatással teszteljen bizonyos döntéseket még azelőtt, hogy a formális csatornákon keresztül közvetítené, s így egyben visszavonhatatlanná is tenné őket. Az sem kizárt, hogy az informális kommunikáció során létrejövő kommunikációs eszközök formalizálódnak, és idővel beépülnek a vállalat hivatalos kommunikációs csatornái közé.

Heidrich (2001) „a szervezeti kultúra elemeinek" részeként, azon belül is a „ceremóniák és szertartások" közé sorolja az ilyen informális kommunikációs csatornát. Eszerint minden szervezetnek szüksége van olyan rendszeresen ismétlődő rendezvényekre, melyek összetartják a dolgozókat, erősítik a kötődésüket a céghez, és nem utolsósorban életben tartják az értékrendet és a tradíciókat. A vezetés nagyon jól használhatja ezeket az alkalmakat az értékek, új elképzelések kommunikálására. Így voltaképpen összecseng a megállapítás a tanulás során tett javaslatommal, hogy nem elegendő évente egyszer oktatni formálisan; ez igaz az informális csatornán közvetített tudásra (normára) is. Tehát tudatos, tervezett módon szükséges megvalósítani, meghatározni, hogy mi legyen a negyedéves, havi hír. Ennek pontos ütemezése, meghatározása a terjedési sebességtől és a szervezet méretétől egyaránt függhet. Másrészt az időszakos vagy rendszeresen tervezett programokban jelenjen meg az információbiztonsági szakterület is.

A kulturális elemek rendszerint az informális kommunikáció csatornáin keresztül terjednek. Ezen az úton értesülhetünk leginkább arról, mi áll a munkavállalók figyelmének középpontjában, mi jellemzi valójában a szervezet jelenlegi helyzetét, illetve mi az, ami várható. Az informális hálózat szerepet játszik az új kollégák eligazításában is azáltal, hogy ezen keresztül ismerhetik meg a különböző múltbeli történeteket, sikereket, tabukat, különböző munkatársak megítélését – ezért a vezetésnek is érdemes figyelembe vennie a hálózat kommunikációját; nem utolsó szempontként a csoportnormaként érvényesülő információátadást, információbiztonsági csoportnormát.

Horváth et al. (2016) szerint a vírusmarketing alatt internetes médiatartalmakba (videókba, képekbe, animációkba, zenékbe, írásos pletykákba) ágyazott tartalmakat értünk, amelyek fő célja, hogy szóbeszédet generáljanak, és a fogyasztók elektronikus szájreklám útján továbbítsák ezeket (érdekes tartalomként, nem pedig reklámüzenetként értelmezve, küldve tovább, osztva meg ezeket saját ismerőseikkel). (Kaizer et al., 2007). A szájreklám (word-of-mouth, WOM), az ismerősök által közvetített reklámüzenet online megjelenési módja, csak abban az esetben képes betölteni funkcióját (a kibocsátó szándékai szerinti üzenet továbbadása a küldő személyes

„hitelének” hozzákapcsolásával), ha az üzenet hiteles, megfogalmazása/megjelenítése eredeti, szórakoztató, és a vírusreklám címzettje közel érzi magához, s felébred benne a vágy arra, hogy megossza az „élményt” ismerőseivel, barátaival. Itt tehát akár a nagyobb tömegekre is hatást gyakorló pletyka egy speciális és gyakran kifejezetten tudatosan használt megvalósulásáról van szó. A WOM részét képezheti a Buzz (más néven pezsgés, zsongás), amely szórakoztató anyagok vagy megragadó hatású hírek alkalmazásával veszi rá az embereket, hogy az adott témáról beszéljenek. (Kaizer, et al., 2007.) A szájreklám mindenhol jelen van, ahol emberek kommunikálnak, magától is fejlődik, a szervezetek azonban sokat tehetnek a fókuszált irányításáért, felerősítéséért. A befolyásoló egyének, véleményvezérek azonosításával vagy rotációs rendszerben megvalósított képzés segítségével tovább fenn lehet tartani az adott témát a napi érdeklődés, beszélgetés, WOM pódiumán. Így az adott információbiztonsági képzés napi aktív tudásban való fenntartása, a felejtési görbének a csillapítása valósulhat meg, akár ezen eszköz segítségével is. Voltaképpen bárhova beágyazhatóak “reklámüzenetek”, adott témában releváns üzenetek, amelyek humorosak, érdekesek, meghökkentők, tehát mindenképpen érdeklődésre tarthatnak számot, szóbeszédet gerjesztenek; majd ezek online platformokon, illetve más digitális csatornákon is vagy eredetileg azokon keresztül terjeszthetőek. (Horváth et al., 2016)

Hennig-Thurau et al. (2004) alapján a szájreklám minden olyan informális kommunikációt jelent, amelynek során a kommunikáció a többi fogyasztó felé irányul, és az információk elsősorban termék vagy szolgáltatás birtoklásáról, használatáról vagy jellemzőiről szólnak. Majd kibővül ez a hagyományos fogalom, és megjelenik az online szájreklám fogalma, amely Hennig-Thurau et al. (2004) alapján minden olyan pozitív vagy negatív állítást jelent, amelyet jelenlegi, potenciális vagy korábbi fogyasztók tesznek közzé egy termékről/szolgáltatásról vagy vállalatról, és amely hozzászólások több fogyasztó számára elérhetőek az internet felületén keresztül. (Horváth et al., 2013)

Horváth et al. (2013) szerint tehát a szájreklám a társas befolyásolás egy típusának tekinthető, és ez a tulajdonság a tradicionális és az online változatot egyaránt jellemzi. “Ezen szemszögből az e-szájreklám a társas kommunikáció egy formájának tekinthető (…), az e-szájreklám az interperszonális kommunikáció kiterjesztéseként is értelmezhető a virtuális térre, amelyben pozitív és negatív információk egyaránt megjelenhetnek, illetve egyszerre jelennek meg az információkereső és az információmegosztó szerepkörök.” (Horváth et al., 2013)

Schnell (2016) az emberi diskurzus összetett természetéről azt írja, hogy ez fontos képesség a társalgás összetett, személyközi helyzetektől, jelentésmódosító elemektől (például a társalgó felek hierarchiája, személyközi célok, személyközi kapcsolatok minősége stb.) átszőtt világában való tájékozódáshoz, s ahhoz, hogy a pragmatikai, vagyis helyzetfüggő jelentéseket a hallgató

sikeresen kikövetkeztesse, és gördülékeny társalgópartnerként vehessen részt az emberi diskurzusban. Ez szintén elengedhetetlen olyan társas célok megértéséhez, melyek nem konkrét, kibontott formában, hanem burkolt (implicit) formában vannak jelen egy társalgásban (ugratás, cinizmus, irónia, hazugság, füllentés, pletyka stb.). Az efféle burkolt célzások és mögöttes szándékaik megértéséhez szükséges a rugalmas pragmatikai kompetencia, mely lehetővé teszi, hogy a sorok között olvasva kikövetkeztessük a szándékolt jelentést, és ennek megfelelően reagáljunk társalgási helyzetekben.

Szász és Kiss (2018) cikkükben az informatikabiztonsági kurzus hatását vizsgálták a hallgatók szokásaira, attitűdjére és mindennapi információbiztonsági tudatosságára, továbbá a kurzus előtt és után kérdőíves felmérést készítettek, s elemezték az alkalmazott oktatási módszereket is. Az elemzés eredményei azt mutatták, hogy a programhasználattal kiegészített, a hallgatói aktivitást facilitáló módszernek jelentősen nagyobb hatása volt a hallgatók információbiztonsági attitűdjére, gyakorlatára és tudatosságára, mint a videóval támogatott oktatási módszernek. Gustavo Percio et al. (2015) összefüggést találtak statisztikai módszerekkel – véleményem egybevág ezen matematikai eredményekkel. Így például azon oktatások segítségével, ahol egy-egy előírás teljes mélységében, a kockázatok részletes és vizuális bemutatásával társult, ott annak kapcsolódási pontjai is mélyebben megteremtődtek, mélyebb elköteleződés, beépülés jött létre. Mindezeket az elveket az általam kidolgozott modellben is érvényesítem.

A nemzetközi szakirodalom áttekintése során számos további befolyásoló tényezőt azonosítottam. A befolyásoló tényezők közül mérvadónak tekintem még az „Elégedettség és motiváció” témakörét, valamint a „Stressz hatása az információbiztonságra”, az „Emberi tévedések, lehetséges hibák” és a „Felhasználói Tudatosság Érettségi Modellje”-nek bemutatását célzó témaköröket is, ez utóbbi a 8. sz. mellékletben szerepel. Sajnos a dolgozat terjedelmi korlátai miatt ezekre itt nem térhetek ki, viszont az általam legjelentősebbnek ítélt négyet: az elégedettséget és motivációt (6. sz. melléklet), a stresszt (7. sz. melléklet), valamint az emberi tévedéseket (9. sz. melléklet), röviden ismertetem, bemutatom.

2.2.6. INFORMÁCIÓBIZTONSÁGI SZABÁLYZATOK

Az adminisztratív intézkedések, például az irányelvek és eljárások, valamint az oktatás és képzés alkalmazásának egyik fő célja az, hogy a munkavállalókat vezesse és ösztönözze a megfelelő biztonsági gyakorlatok betartására (például ne ossza meg jelszavait vagy ellenőrizze a gyanús e-mail-mellékleteket, mielőtt megnyitná). Valójában a szervezeti biztonsági problémák többségét

közvetett módon azok a munkavállalók okozzák, akik megsértik vagy elhanyagolják szervezetük információbiztonsági szabályzatát. Ennek következtében ebben az alfejezetben a szabályozás kérdésével foglalkozom. Az is fontos kérdés, hogy az egyes szerepkörökben dolgozó munkavállalók vagy külső felek (stakeholderek) hogyan érzékelik az információbiztonsági szabályzatot és követelményrendszert, és milyen az erről szóló kommunikáció. (Spyridon Samonasa et al., 2020). Levin (2018) állítja, a biztonsági politikák közértehetelenségének egyik oka az, hogy a megfeleléshez gyakran nagyon hosszú szövegek társulnak, amelyeket nem mindenki olvas el. Például az Intel-alapú számítógépek sebezhetősége esetében a szoftvermérnököknek el kellett volna olvasniuk egy 4844 oldalas dokumentumot, hogy biztosítsák az Intel biztonsági előírásainak való megfelelést.

A magyar szabályozástól a nemzetközi irányába haladva elsőként a magyar jogszabályi, majd nemzetközi szakirodalmat tekintem át.

A Kormány e-kormányzati stratégiájában kiemelt szerepet szánt a nemzetbiztonság és ezen belül is a kibervédelem szempontjainak. Ebbéli szándékának megfelelő törvényi hátteret is teremtett, mely figyelemreméltó szisztematikussággal alapozza meg e szempontok érvényesülését. Elsőként a „Magyarország Nemzeti Biztonsági Stratégiájáról szóló 1035/2012. (II. 21.) Korm. határozatot" fogadták el, amelynek 31. pontja szól a kiberbiztonságról (kihirdetve: Magyar Közlöny 2012. évi 19. szám). Ezt követte a kiberbiztonság részletesebb kifejtését tartalmazó dokumentum, a „Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. határozat" (kihirdetve: Magyar Közlöny 2013. évi 47. szám). E stratégiai dokumentumok kimunkálását és elfogadását követte az első jogalkotási lépés, „Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvény" (a továbbiakban: Ibtv.) elfogadása (kihirdetve: Magyar Közlöny 2013. évi 69. szám). A törvényben meghatározott célok és feladatok végrehajtását részterületenként határozta meg még részletesebben egy sor rendelet, melyek közül témánk szempontjából a legfontosabb, „Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló törvényben meghatározott vezetői és az elektronikus információs rendszer biztonságáért felelős személyek képzésének és továbbképzésének tartalmáról szóló 26/2013. (X. 21.) KIM rendelet" (kihirdetve: Magyar Közlöny 2013. évi 173. szám).

A Kiberbiztonsági Stratégia célja „a szabad és biztonságos kibertér kialakítása és a nemzeti szuverenitás védelme". Ezen belül a stratégia célja, hogy a magyar kibertér mint a gazdasági és társadalmi élet meghatározó területe, egyszerre legyen szabad, biztonságos és innovatív. A Stratégia nemzetközi dokumentumok által is erősen körbebástyázott. Alapelveiben és alapértékeiben három fő nemzetközi forrásra támaszkodik:

1) szakmai sztenderdekre, mint a 2001-ben elfogadott Budapesti Konvenció („Convention on Cybercrime”);
2) az EU vonatkozó dokumentumaira, mint az Európai Parlament által 2012. november 22-én elfogadott, „A kiberbiztonságról és védelemről szóló” 2012/2096(INI) számú határozatban a tagállamok felé megfogalmazott ajánlásokra, valamint az Európai Bizottság és az Európai Unió közös kül- és biztonságpolitikájának főképviselője által 2013. február 7-én „Az Európai Unió Kiberbiztonsági Stratégiája: egy nyílt, biztonságos és megbízható kibertér” címmel közzétett közös közleményre;
3) valamint a NATO vonatkozó megállapodásaira, különösen a 2010 novemberében elfogadott Stratégiai Koncepcióra, a 2011 júniusában elfogadott Kibervédelmi Politikájára, valamint a 2010. november 19-20-ai lisszaboni és a 2012. május 20-21-ei chicagói NATO-csúcs dokumentumaiban megfogalmazott Szövetségi kibervédelmi elvekre és célokra.

A Stratégia a magyar kiberteret a globálisan összekapcsolt információs rendszerek azon részeként definiálja, amelyekben a keletkező adatok és információk vonatkozásában Magyarország valamilyen formában érintett. A Stratégia részletesen leírja azokat a célokat, irányokat, feladatokat és eszközöket, amelyeken keresztül a magyar kormányzat biztosíthatja a magyar kibertér védelmét, a technológiai innovációk adaptálását és a szorosabb nemzetközi együttműködést. Az egész stratégia egyik legfontosabb üzenete a megelőzés, az oktatás és képzés, valamint a biztonsággal kapcsolatos tudatosság fontosságának hangsúlyozása, mely az egész dokumentumban visszatérő elem. Ezen felül a közigazgatást és az e-kormányzati rendszereket is mint a kibervédelem elsődleges prioritással rendelkező területeit említi a dokumentum: „Magyarország kiemelt figyelmet fordít arra, hogy az általános, a közép- és felsőoktatásban, a kormányzati tisztviselők képzésében és a szakmai továbbképzéseken a kiberbiztonság szakterülete integrálódjon az informatikai oktatásba. Magyarország stratégiai együttműködés kialakítására törekszik azon egyetemi és tudományos kutatóhelyekkel, melyek a kiberbiztonsági kutatás-fejlesztésben kiemelkedő és nemzetközileg is elismert eredményeket mutatnak fel, és segítik a kiberbiztonsági kiválósági központok kialakulását” – fogalmaz a Stratégia. A teljes kép bemutatása érdekében disszertációm 10. sz. mellékletében kitérek az Európai Unió, így Magyarország számára információbiztonsági szempontból jelentős szervezet (ENISA[2]), valamint

[2] ENISA: European Union Agency for Cybersecurity – Az Európai Unió 2004-ben hozta létre European Network and Information Security Agency néven.
Forrás: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML

az információbiztonsághoz és szorosan vett informatikai irányításhoz kapcsolódó tanúsító szervezetek és tanúsítványok rövid bemutatására is.

A Kiberbiztonsági Stratégiában elfogadott célok és elvek mentén született meg "Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló" 2013. évi L. törvény (Ibtv.), amely a közigazgatás szinte minden szintjén új feladatokat határozott meg. A törvény alapvető célja a „nemzeti vagyon részét képező nemzeti elektronikus adatvagyon, valamint az ezt kezelő elektronikus információs rendszerek, illetve a létfontosságú elektronikus információs rendszerek és rendszerelemek biztonságának" védelme. A törvény, miután tisztázta a kiberbiztonsággal kapcsolatos legfontosabb fogalmakat, a törvény intézményi hatályát határozta meg. Eszerint a kormányzati elektronikus információbiztonság az alábbi intézményeket érinti:
a központi államigazgatás szerveit a Kormány és a kormánybizottságok kivételével;
a Köztársasági Elnöki Hivatalt;
az Országgyűlés Hivatalát;
az Alkotmánybíróság Hivatalát;
az Országos Bíróság Hivatalát és a bíróságokat;
az ügyészségeket;
az Alapvető Jogok Biztosának Hivatalát;
az Állami Számvevőszéket;
a Magyar Nemzeti Bankot;
a fővárosi és megyei kormányhivatalokat;
a helyi és a nemzetiségi önkormányzatok képviselőtestületének hivatalait;
a hatósági igazgatási társulásokat;
a Magyar Honvédséget.
A törvény hatálya alá tartoznak a felsorolt intézmények számára adatkezelést végzők is csakúgy, mint a nemzeti adatvagyon körébe tartozó állami nyilvántartások adatfeldolgozói, valamint a törvény alapján európai és nemzeti létfontosságúvá kijelölt rendszerelemek. A törvény alapján tehát ez az a szervezeti kör, amelynek munkatársait elektronikus információbiztonsági képzésben kell részesíteni. A törvény és annak nyomán megszületett 26/2013. (X. 21.) KIM rendelet három szinten nevezi meg azokat a közigazgatásban dolgozó alkalmazottakat, akiknek képzéséről gondoskodni kell: EIB (elektronikus információbiztonsági) felelős vezető, EIB résztvevő és EIB felelős.

A kérdőívre adott válaszok értékeléséhez le kell szögezni, hogy az informatikai biztonság egy olyan terület, amely „nem mérhető jól" kérdőívvel. Ennek két oka van. Az egyiket fentebb már említettük: Sokan a kérdésfeltevés analógiájára próbálnak logikusan, szándékuk szerint

helyesen válaszolni. Tehát igazi pontos mérés akkor keletkezne, ha éles helyzetben derülne ki, hogy valóban úgy is cselekszik-e a munkavállaló, mint ahogy elméletben tudja vagy sejti a jó választ. A tréning és a gyakorlati alapon szerzett tudás is rendkívül fontos. Hiszen ez mutatja meg, egy tesztelés, egy-egy éles helyzet esetén hogyan képes szervezeti vagy nemzeti szinten kezelni az eseményt. Nem csak Magyarországi, de nemzetközi szinten vizsgálva is kirajzolódik, hogy nemzeti szinten is fontos tényezőként tekintenek a kiberbiztonsági politikákra. (Kovács, 2012) Azaz ez az egész Európai Unióban és szélesebb körben is észlelt jelenség a kiberterrorizmus, amire nemzeti szinten is reagálnak az egyes országok. Ezzel természetesen nem a kérdőíves felmérés ellen érvelek, hanem azt kívánom hangsúlyozni, hogy mindegyik módszernek megvan a helye és szerepe.

A másik fontos oka annak, hogy nehéz mérni egy szervezet informatikai biztonsági szintjét az, hogy a kérdőíves kutatások logikájának megfelelően nem a teljes alapsokaságot szondázzuk, hanem azokból valamilyen módszer szerint mintát veszünk. Holott az információbiztonság egyik legfontosabb célkitűzése mindig az „egyenszilárdság" megteremtése. Egy példával illusztrálva ez azt jelenti, hogy ha százból csak egyetlen felhasználó hagyja nyitva a munkahelyén a bejárati ajtót, akkor azon ugyanúgy be tudnak menni a (adat)tolvajok, mintha 99 hagyta volna nyitva. Tehát, ha egyetlen számítógépet sikeresen megfertőznek célzott vagy véletlen támadás során, akkor onnan már könnyedén, de legalábbis könnyebben tudják a szervezet többi számítógépét, szervereit célba venni. (Illéssy, Nemeslaki, Som, 2014)

További fontos megállapítás, hogy tökéletes biztonság nem létezik, de a szervezet erőforrásaihoz képest erre kell törekedni. A ráfordítások és a biztonsági szint arányban tartása és ezen arány eldöntése mindig az adott szervezet vagy intézmény feladata és felelőssége.

A nemzetközi szakirodalmi áttekintésnél talán az *érdekelt felek* fogalma az egyik kulcsfogalom. Az érdekelt felekbe voltaképpen minden olyan szereplőt (egyént, céges partnert, beszállítót) szükséges beleérteni, aki valamilyen formában szerződéses, jogi, egyéb kapcsolatban van a szervezettel, annak információbiztonsági állapotára hatással lehet, vagy egy ilyen hatás van rá hatással. Cram et al. (2017) szerint az érdekelt felek felfogásának megértése kulcsfontosságú kérdés, amely a biztonsági politikák kétszintű kidolgozásához kapcsolódik. Az első a biztonsági politikát magában foglaló specifikus szabályok kiválasztását érinti. A hatékony biztonsági politikában az abba foglalt szabályoknak összhangban kell lenniük a szervezet műszaki képességeivel, üzleti folyamataival és kultúrájával. (Dhillon, 2007; Goel és Chengalur-Smith, 2010) Az érdekelt felek eltérő érdekei és a biztonsági szabályzattal való interakciója befolyásolja a szabályzat felfogását; ezek a felfogások viszont hozzájárulnak a szabályzat végső sikeréhez vagy kudarcához. (Bauer et al., 2017; Chen et al. 2015; Niemimaa et al., 2013)

Másodszor, és szorosan összekapcsolódva az első szinttel, a biztonsági politika sikeres végrehajtása az előírt szabályok hatékony kommunikációjától függ az érintett szervezeti érdekelt felek között. Mint Niemimaa és Niemimaa (2017) megjegyzik, ez egy kihívást jelentő folyamat lehet, amely a globális szabványok és a bevált gyakorlatok átvételével és "átfordításával" kezdődik. A globális szabványok és a bevált gyakorlatok követelményeinek konkrét és megvalósítható biztonsági szabályokként történő átalakítását kommunikálni kell és közzé kell tenni a szervezeten belül. (Niemimaa és Niemimaa, 2017) Ezért nem elegendő csak hangsúlyt fektetni egy biztonsági irányelv, dokumentum teljességére vagy a felhasználói megfelelés biztosításának szükségességére; inkább ki kell egészíteni a szervezeti érdekeltek biztonsági politikával kapcsolatos felfogásának alapos megértésével Niemimaa et al. (2013) szerint. Kutatásaim is alátámasztják, hogy az információbiztonsági szabályzat közzététele önmagában nem jelenti az, hogy másnaptól tudomásuk lesz róla, alkalmazni fogják tudni. Azaz a szabályzat életciklusa során például, de nem kizárólag, figyelembe kell venni:

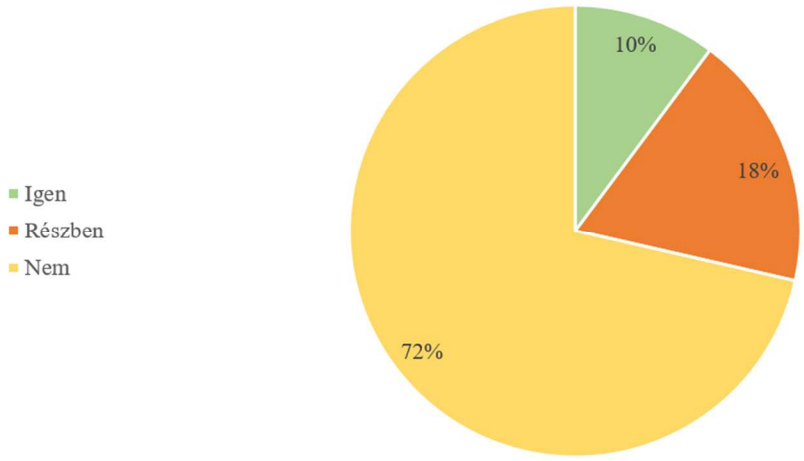
- a szerepkör alapú kidolgozást (user involvement),
- a szabályzat megfelelő kommunikációját,
- a bevezetési időablakot, amely az átálláshoz nyújt támogatást,
    - megfelelő informatikai és
    - megfelelő információbiztonsági támogatást
- a szabályzat folyamatokban való alkalmazásának támogatását,
- egyéb szempontokat.

Buthelezi et al. (2016) rámutatott a biztonságpolitikai dokumentumok félreérthetőségére és azok téves értelmezésére mint a biztonsági szabályok be nem tartásának egyik fő okára. A hatékony informatikai rendszer (információbiztonsági szempontokat is figyelembe véve) fenntartása érdekében az állandóan változó kiberbiztonsági környezetben a szervezetek folyamatos biztonsági előírásokat követelnek az alkalmazottaktól. Így a munkavállalói megfelelési tevékenységek kritikusak a számítógépes rendszerek biztonságának fenntartása szempontjából. Ugyanakkor a felhasználók alacsony motivációja a biztonsági politikák betartására a biztonság megsértésének (security breaches) több mint 40%-ához vezet. (Johnston, et al. 2015) Egy biztonságos kiberbiztonsági rendszer érdekében a munkavállalók hozzáállása, megítélése az információbiztonsági követelményekkel kapcsolatban kiemelten fontos. (Kraus et al., 2017) Ezenkívül a felhasználók tudása és készségei is fontosak, ezért más kutatások feltételezése az, hogy a jobb biztonsági ismeretekkel rendelkező és kockázattudatos emberek nagyobb

valószínűséggel fogják betartani a biztonsági politikákat; továbbá, ha tartanak a megsértésből eredő szankcióktól, kevésbé valószínű, hogy megsértik a biztonsági politikát. (Guo, Yuan, 2012)

Az információbiztonsági szabályzat felhasználók által észlelt minősége és hasznossága pozitívan befolyásolta a tényleges biztonsági előírások betartását. (Pahnila et al., 2007) Ugyanakkor a munkavállalók a frusztráció egy forrásaként gyakran a hagyományos írásbeli informatikai és biztonsági politikákhoz való hozzáférés szükségességével indokolták. Pham HC et al. (2016) azt is megállapította, hogy az írásbeli irányelveknek (written policies) nem volt sok hasznuk a biztonsági gyakorlati útmutatás nyújtásában, és hosszabbnak és nehezen olvashatónak tekintették őket az ismeretlen kifejezések használata miatt.

Kutatási tapasztalataim alapján továbbá kiemelem, hogy az általam megvizsgált, információbiztonsági szabályzatot tartalmazó dokumentumok több, közel ¾-e nem volt kereshető. Azaz a dokumentumon belül nem lehetett szavakra rákeresni. Ez megnehezíti a szabályzat feldolgozását az adott munkakörre releváns ismereteket kereső munkavállaló számára. Összesen 49 darab szervezetnél vizsgáltam meg információbiztonsági szabályozó dokumentumot környezetet, amelyek eredményét a 6. sz. ábrán mutatom be.



7. ábra: Az információbiztonsági szabályzatokban való kereshetőség (%), forrás: saját szerkesztés

A 7. számú ábrán látható, hogy a dokumentumok 72%-ában nem lehetett kulcsszavak szerint keresni. Azaz ezen dokumentumokat esetében az egészet szükséges végigolvasni egy-egy releváns mondat érdekében, például, ha az előírt jelszóhosszra mint információra van szüksége egy stakeholdernek. Általában véve belátható, hogy egy elektronikus könyv ilyen jellegű elérhetősége, kereshetősége jelentősen meghatározza annak használhatóságát. A fenti ábrán az látható, hogy a vizsgált szervezetek 10%-ánál volt csupán kereshető az információbiztonsági szabályzat. A dokumentumok 18%-a részben volt kereshető, ami azt jelenti, hogy némely rész

képként vagy szkennelt anyagként állt rendelkezésre, amiben nem volt a keresés kivitelezhető, így a felhasználó egyes kérdéseire csak hosszabb keresgélés és olvasgatás után kaphat választ. Azaz a túlnyomó többségben (90%) nem ill. részben kereshető dokumentumok véleményem szerint azt is eredményezik, hogy nehezebb vagy egyáltalán nem találja meg az adott kereső személy a releváns (rá, a munkafolyamataira vonatkozó) dolgokat, előírásokat ami miatt nem is fogja tudni követni a számára előírt szabályokat.

A felhasználók nagyobb valószínűséggel hajtják végre a biztonsági tevékenységeket, amikor megértik a biztonsági program céljait, amikor úgy látják, hogy a biztonsági intézkedések relevánsak és hatékonyak a kockázatokkal szemben, és amikor úgy vélik, hogy képesek ilyen feladatokat végrehajtani. (Vance A., Siponen M., 2012).

A disszertációmban már említett SRS (security related stress) csökkentésének lehetséges mechanizmusai közül a legnyilvánvalóbbak a pontosan és egyértelműen megfogalmazott (azaz nincs túlzott technikai zsargon és jogi fogalmak) biztonsági szabályzatok, amelyek részletes megfelelőségi eljárásokat tartalmaznak. Az ilyen szabályzatoknak enyhíteni kell a biztonsági követelmények észlelt összetettségét, különös tekintettel a nem műszaki személyzet esetében. A szervezetek hatékonyan küzdhetnek meg a biztonsággal kapcsolatos összetettséggel is olyan időszakos biztonsági oktatás, képzés és tudatosságprogramok (security education, training and awareness, SETA) segítségével, amelyek a legújabb biztonsági és műszaki ismereteket közvetítik. A biztonsági követelményekkel kapcsolatos bizonytalanság csökkentése érdekében a SETA programok tartalmazhatnak egy olyan összetevőt, amely leírja a jelenlegi szabályozási környezetet és a közelgő biztonsági irányelvi (adminisztratív és technikai) változásokat, hogy az alkalmazottak felkészülhessenek arra, hogy beillesszék munkarendjükbe. A szervezetek bevonhatják az alkalmazottakat a biztonsági követelmények megtervezésébe és végrehajtásába is, mint az SRS csökkentésének egy eszközeként. Példa erre az új biztonsági követelmények tesztelése, visszajelzés nyújtása a vezetőség számára és a biztonsági változások kommunikálása a munkatársakkal. (Salanova et al., 2000) A munkavállalók ilyen módon történő bevonásával csökkenteni lehet bennük a bizonytalanságot. Mivel az alkalmazottak jobban tájékozódnak arról, hogy miért jelentkeznek új biztonsági követelmények, csökkenteni lehet a komplexitás érzetét is, mivel az alkalmazottaknak lehetősége nyílik megismerkedni a biztonsági követelményekkel, még mielőtt azok teljeskörűen végrehajtásra kerülnének; emellett, ha az alkalmazottak valamilyen befolyást gyakorolnak a biztonsági követelmények megtervezésére és végrehajtására, akkor a követelményeket kevésbé ellentétesnek kell érezniük a termelékenységgel. Ez csökkenti a túlterhelés érzetét, és a szerepkörök, folyamatok jobb megértését és jobb információbiztonsági

szabályzat és gyakorlat kialakítását eredményezheti az információbiztonsági szakterület felé adott visszajelzések alapján.

A SETA (security education, training and awareness) kifejezést szakirodalmi áttekintésem alapján Whitman (2004) alkalmazta elsőként. Whitman szerint a SETA program három elemből áll: biztonsági oktatás (education), biztonsági képzés (training) és biztonságtudatosság (awareness). Ugyanakkor megjegyzi, hogy előfordulhat, hogy ha egy szervezet nem képes vagy hajlandó mindhárom elemre vállalkozni, akkor esetleg részben vagy egészben kiszervezhető. Tapasztalataim szerint ez nem túl elterjedt még a magyar közigazgatásban. A SETA céljai:

- a rendszererőforrások védelmének szükségességével kapcsolatos tudatosság növelése;
- készségek és ismeretek fejlesztése, hogy a számítógép-felhasználók biztonságosabb munkát végezhessenek;
- szükség esetén mélyreható ismeretek építése a szervezetek és rendszerek biztonsági programjainak tervezéséhez, megvalósításához vagy működtetéséhez.

Ugyanakkor két jelenségre lettem figyelmes: a *SETA program* kifejezés használata kevésbé elterjedt (kevésbé ismert), mint annak egyik összetevője, *az awareness education*, biztonságtudatossági oktatás. Azaz egyelőre a nemzetközi szakirodalomban is kevésbé elterjedt, hogy a gyakorlatba ültetett szabálykövetéshez több komponens szükséges, mint csupán szabályzat vagy valamilyen (frontális, egyirányú) oktatás. A *Security Awareness, Training and Education* (SATE) és az *Awareness and Training* (AT) 1995 októberében lett publikálva. (NIST, SP 800-12, 1995.) Itt, bár a szóhasználat még közel azonos volt, ezen rövidítés nem jelent meg, csak az *AT*, *awareness training*, illetve más volt a szórend.

Ezt követően, véleményem szerint azért, mivel Whitman könyv és nem cikk formájában, a tudományos adatbázisokban nehezebben vagy részlegesen hozzáférhető volt, a kifejezés átkerült a tudományos szóhasználatba, de annak pontos és részletes értelmezése már csorbát szenvedett.

Kesh és Ratnasingam (2007) több rétegbe különíti el az információbiztonsági szabály alkalmazhatóságához, tudatossághoz szükséges rétegeket (Information Security Knowledge Architecture, ISKA):

- Információbiztonsági tervezés (Information Security Planning)
- Információbiztonsági szabályzat fejlesztése (Information Security Policy Development)
- Információbiztonsági projektmenedzsment (Information Security Project Management)
- Biztonságirányítási architektúrák, modellek és gyakorlatok (Security Management Architectures, Models, and Practices)
- Kockázatkezelés az IT-biztonságban (Risk Management for IT Security)

- Védelmi mechanizmusok (Protection Mechanisms)
- Személyzet és biztonság (Personnel and Security)
- Jog és etika (Law and Ethics)

Valamint Kesh és Ratnasingam (2007) alapján az információbiztonsági tudás, alkalmazás típusa és szintje szerint definiálta az egyes szinteket, melyet az alábbi táblázatban foglaltam össze:

Az információbiztonsági tudás, a tudásalkalamzás típusa, vagy szintje.	Definiciók	Az információ biztonság tudásdimenziói
Deklaratív, kinyilatkoztató	Tudni róla	Annak ismerete, hogy milyen biztonsági intézkedések vannak, amelyek képesek kiküszöbölni és csökkenteni a kockázatokat. Például: Titkosítási technológiák megléte.
Eljárási	Tudni hogyan	A biztonsági irányelvek és eljárások megosztásának ismerete az összes alkalmazott számára. A tudás egyértelmű és nyilvánosságra kerül. Például: Hogyan lehet a titkosítási technológiákat megvalósítani?
Egyedi / Egyéni	Az egyén alkotta és benne rejlik (hallgatólagos tudás)	Az érdekelt feleknek (informatikai vezetőknek, biztonsági elemzőknek és biztonsági adminisztrátoroknak) tisztában kell lenniük a hatékony kockázatkezelés biztonsági intézkedéseivel. Például: Az egyes érdekelt felek rendelkeznek ismeretekkel a titkosítási technológiákról.
Társadalmi	Létrehozta és benne rejlik egy csoport kollektív cselekedeteiben.	Az érdekeltek csoportjai, amelyek meghatározzák a biztonsági irányítás érdekében végrehajtandó kollektív intézkedéseket. Például: Hogyan tudják az érdekeltek csoportjai megvalósítani és megosztani az információs technológiák ismereteit?
Feltételes	Tudni mikor	Az érdekelt feleknek ismerniük kell, hogy mikor kell alkalmazni a biztonsági ellenőrzéseket és intézkedéseket. Példa: Melyik titkosítási technológiát kell használni és mikor?
Relációs	Tudni mivel	A rendszer biztonságának fenntartásában részt vevő alkalmazottaknak jól képzettnek kell lenniük annak érdekében, hogy képesek legyenek kellő időben kommunikálni más biztonsági adminisztrátorokkal. Például: Melyik csoportok kapcsolódjanak egymáshoz és osszák meg a titkosítási technológiák ismereteit?
Gyakorlatias	Hasznos ismeretek a szervezetről	Naprakész, jó üzleti gyakorlatok és biztonsági irányelvek létrehozása. Például: Milyen szervezeti irányelveknek kell irányitaniuk azt, hogy mely titkosítási technológiákat valósítsák meg, illetve mikor és hogyan? Saját folyamataiban alkalmazni tudja az előírásokat.
Kezdeményező	Proaktívan alkalmazza, érvényesíti és példát mutat. Szükség esetén jelenti az események és támogatást kér.	Ha valamely új lefedetlen kérdéskör merül fel, akkor azt jelzi.

1. táblázat: Az információbiztonsági tudás, tudásalkalmazás szintjei, forrás: Kesh és Ratnasingam (2007) alapján

A táblázatból leolvasható, hogy nem a klasszikus 5 fokozatú skálát alkalmazza, amely talán egy jobb, részletesebb beosztást tesz lehetővé. Ezt egészítettem ki az utolsó sorban a proaktív, kezdeményező típussal, amely nem csak alkalmazza a megtanult gyakorlatokat, de proaktívan viszonyul a helyzetekhez. Ezek a kivételek kezelése és a türelmi idő kérdései.

A szabályzatokról szóló nemzetközi szakirodalom áttekintése kapcsán természetesen voltak egészen egzotikus teóriák is. Ugyanakkor szakmai tapasztalataim alapján két területet szinte csak említés szintjén találtam meg, melyek ugyanakkor szerintem egy jól működő szabályozáshoz szükségesek.

A kivételek kezelésének lehetősége és módszertana, valamint a szabályzat változása vagy bevezetése során annak ütemterve, úgymond a türelmi idő kérdésköre nem jelenik meg sem a magyar, sem a nemzetközi szakirodalomban.

Andress és Leary (2017) úgy fogalmaz, hogy az információbiztonsági szabályzat kell, hogy tartalmazzon kivételkezelést, és hogy azt alkalmazni lehessen, amikor helyénvaló. A szabályzatnak természetesen rögzítenie kell egyértelmű irányelveket, de meg kell adnia azt a folyamatot, hogyan lehetséges a kivételek kezelése, világosan megfogalmazva és azt betartatva, ugyanakkor ezáltal biztosítva a kivételek kezelésének mechanizmusát a szabályzat gyengítése nélkül. Disszertációmban számtalanszor utaltam a koherens viselkedésre, a szabálykövetési hajlandóságra, így voltaképpen a kivételkezelés hiánya esetén a szabályzattal szemben történő megoldás az egyén szabálykövetési hajlandóságát is csökkentheti, mivel egyszer már szabályzatot kellett, hogy szegjen. Ugyanakkor azok az alkalmazottak, akik az információbiztonsági szabályzatnak való megfelelés kihívásával néznek szembe, választhatják, hogy teljesen figyelmen kívül hagyják-e a szabályzatot, vagy a szabályzatban szereplő kivételes záradékot alkalmazzák. Kivételkezelés nélkül a munkavállaló egyszerűen az egész szabályzatot, a teljes szabálykövetést adhatja fel.

Seymour et al. (2008) szerint útmutató is szükséges a kivételek engedélyezéséhez. Minden szabálynál elkerülhetetlenül vannak kivételek. Abban az esetben, ha a felhasználó kivételt kér egy szabály alól, a kérelmek feldolgozására, felülvizsgálatára, jóváhagyására vagy elutasítására eljárásnak kell lennie. Ez a szakasz meghatározza, hogy ki, mikor és hogyan végezzen egy ilyen eljárást.

A másik fentebb említett, az információbiztonsági szabályzatokból indokolatlanul hiányzó terület a türelmi idő kérdésköre. Andress és Leary (2017) talán kissé viccesen úgy fogalmaz, hogy a cégek nem válnak egyik napról a másikra megfelelővé az előírt információbiztonsági szabályzatnak. A türelmi idő egy elfogadott periódust biztosíthat, amíg a megfelelőség vizsgálata, mérése meg nem kezdődik. Így az adott szakterületeknek van ideje az elvárásokat kommunikálni, oktatni, alkalmazni, ahol lehetséges (vagy ott alkalmazni, ahol lehetséges), és a formális vizsgálatok (pl.: belső audit) előtt megbizonyosodni annak eredményességéről. Így az információbiztonsági szabályzat kiadása, frissítése alkalmával, az új előírás megjelenésekor ahhoz igazítható és kommunikálható a belső audit terv, a meghatározott türelmi időhöz igazítva. A türelmi idő jellemzően néhány hónaptól egy évig terjedhet.

Megítélésem szerint ezen két terület hiánya jelentősen hozzájárulhat az információbiztonsági szabályzatok és ezáltal a információbiztonsági szabálykövetési hajlandóság degradációjához. Mivel nem lehetséges egy szabályzatban minden életszerű eseményt leírni, így

szükséges a kivételkezelés hivatalos bejáratott formáját létrehozni. Másrészről nem lehetséges, nem életszerű egyik napról a másikra egy előírást kommunikálni, oktatni és a gyakorlatban felkészíteni rá a munkavállalókat; ez magában hordozza a szükségszerű szembekerülést a szabályzattal, aminek akár a teljes információbiztonsági szabálykövetési hajlandóság megszűnése, vagy feladása is lehet a következménye.

2.2.7. MÉRÉS, EGYÉNI ÉS SZERVEZETI TUDATOSSÁG SZINTJEI

A *Magyar értelmező kéziszótár* a „mérés" szót a következőképp definiálja:

mér A ts ige 1. (t. n. is) (Nagyságot) számokban meghatároz(ni igyekszik).

mérés B fn 1. Az a cselekvés, hogy vki mér vmit. |

A *Magyar szinonimaszótár* szerint:

mér

A [hosszasan, ismételten] méreget, [aprólékosan] méricskél; [versenyzők testsúlyát, ill. hivatalos szállítmányt, rakományt] mérlegel, [rendszerint nagyobb súlyt, mázsán, (tizedes) mérlegen:] lemázsál, mázsál; méri magát: bizalmas: megméredzkedik, méredzkedik, megméretkezik, méretkezik; [mélységet, szondával] szondáz; [hőmérsékletet, lázmérővel] hőmérőz; bizalmas [időt, stopperórával] stoppol

B [árucikkből, anyagból bizonyos mennyiséget:] kimér, lemér; nyelvjárási [árucikket: jól, bőven] megmér, [eladva] → árul

C [valamit (valamiből) valakinek juttatva:] osztogat, oszt

D [valaminek a nagyságát valamihez] szab

E [valakihez, valamihez] → összehasonlít valakivel, valamivel

F [ütést, csapást, büntetésül valakire] rámér, [ütést, vágást] → ad valakinek ‹tágabb értelmű›

G választékos [(terhes) feladatot, kötelességet, büntetést] → ró

A mérés tehát valamilyen számszerűsítést, kvantifikálást kell, hogy jelentsen. Ez maga a kiindulási probléma, hogy az ember, a munkavállaló információbiztonsági tudatossági szintje vagy egy adott munkaszervezet információbiztonsági tudatossági szintje közvetlenül nem mérhető meg oly módon, mint az SI mértékegységben.

A következő megválaszolandó kérdés a mérés témakörében, hogy a tudatosságot milyen szinten próbáljuk mérni. Mérési lehetőségeket a következő szinteken találhatunk:

- Az egyén szintjén
- A (tudatosító) programok szintjén
- Szervezeti szinten

Mindhárom szintre igazak a fenti kvantifikálással kapcsolatos megállapítások:

- Az egyén szintjén végzett mérés nem közvetlen mérés, és egy időbeli lenyomatot képes csak visszaadni. Ugyanakkor előfordulhat, hogy maga a mérés is befolyásolja a mérendő személyt.
- A programok szintjén folyó mérés nem ad teljes képet a szervezet egészének tudatossággal kapcsolatos működéséről, hanem csak egy önkényesen kiválasztott szelete, a programmenedzsment (IS governance) kerül vizsgálat alá. (Tarján, 2002)
- A szervezeti szinten zajló mérés az egyértelmű mérőszámok hiányától kezdve a mérőszámok számosságának meghatározásáig, a lehetséges al- vagy kapcsolódó mérőszámok végtelen számosságáig, sok érték kiértékeléséig és méréselméleti kérdésekig hordoz kihívásokat.

Természetesen ez leegyszerűsítése a kérdésnek, hiszen további köztes szintek is lehetnek, például a szabályalkalmazás képessége vagy ennek mérése szimulációs tesztben. Illetve az is elképzelhető, hogy az információbiztonság egyes területein eltérő ismeretekkel és eltérő tudatossági szintel, tudással rendelkezik.

Az egyén mérését talán úgy érdemes kezelni, hogy észlelt szabályzatszegés esetén (automatizált, automatizáltan kiutalt) oktatáson szükséges részt vennie, természetesen az ügy súlyától függően. Az éves képzési tervben (és/vagy a fegyelmi szabályzatban is) szükséges ezeket előre definiálni. A szervezeti szinten zajló mérés segíthet a személyes konfliktusok elkerülésében, és egyéb előnyöket is kínál a szervezet számára (Tarján, 2020):

- A szervezet mint egész egy holisztikus képet kap az információbiztonsági tudatosság szintjéről.
- Az információbiztonsági vezetők világos képet kapnak arról, hogy hol vannak hiányzó vagy rosszul működő kontrollok vagy lehetőségek a továbbfejlesztésre.
- Milyen lehetséges automatizmusokkal lehetne a felhasználói viselkedést támogatni?
- Milyen megoldásokkal lehet a biztonsági előírásokat a munkafolyamatokhoz illeszteni?

Muha (2009) tanulmányában, részben a NIST szabvány, az SP800-55-re hivatkozva megfogalmazza, hogy

- a méréseknek mennyiségi információt kell nyújtaniuk (százalékok, átlagok, és számok);
- a mérések alapjául szolgáló adatoknak könnyen használhatónak kell lenniük;

- csak megismételhető informatikai biztonsági eljárások vehetők figyelembe a mérések során;

  és

- a méréseknek hasznosíthatónak kell lenniük a teljesítmény értékeléséhez és az erőforrások kezelésében.

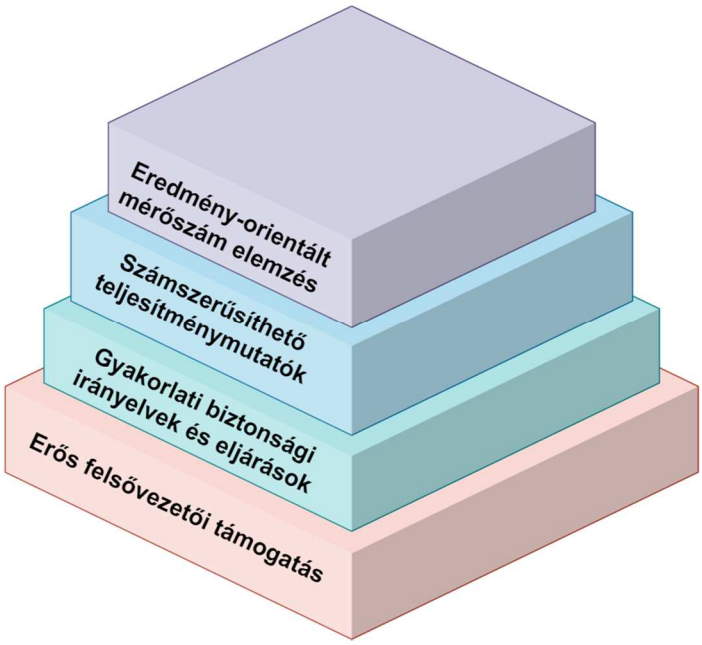
Az első pont az összehasonlíthatóságra vonatkozik a skálatulajdonságok figyelembevételével.
A második pont lényege, hogy felgyorsult világban gyors válaszok és eredmények szükségesek, gyakran nem opció vagy megoldás a kézi kiértékelés, így automatizálható értékekre van szükség.
A harmadik pont ezekből következik, azaz idősorosan rendelkezésre álló adatokra szükséges törekedni, ugyanazokat a méréseket rendszeresen végrehajtva.
A negyedik pont a relevancia, azaz a mérésnek felhasználhatónak kell lennie, hogy arra képes legyen a szervezet reagálni, azt hasznosítani.
Tehát megállapítható, hogy az egyes munkavállalók közvetlenül nem mérhetőek. Ugyanakkor számos egyéb módon rendelkezésre álló adatokból, viselkedésből vagy elektronikus rendszerekből származó, illetve kérdőíves módon kapott adatok révén az egyének kvantifikálhatóak, azaz számadatokat kaphatunk.
A szervezeti szintű mérést leginkább az érettségi modellek támogatják. Az Information Security Awareness Capability Model (ISACM), melyet Poepjes és Lane (2012) publikált a COBIT vagy ITIL-ben, szintén az ismerősen csengő 5 fokozatú skálát veszi alapul:
Initial: nincs awareness program,
Repetable: megfelelőségre fókuszáló,
Defined: támogatja a tudaságot és a változást,
Managed: hosszú távú a fenntartása
Optimizing: mérhető keretrendszerben

Az ISACM a tudatosság három fontos dimenzióját határozza meg: a fontosságot, a döntésképességet és a kockázatot. Ugyanakkor létrehozza az érdekelt felek csoportjait is (IT személyzet, vezetők és végfelhasználók). Ez a csoportosítás azonban rögtön jól mutatja a modell lehetsőségeinek a korlátait is: Csak az informatika szemszögéből tekint a tudatosságra (holott az információbiztonsági tudatosság nem csak az informatikáról szól), és a külső érdekelt felek egyáltalán nincsenek figyelembe véve ebben a modellben.

Az informatikai biztonsági metrikák végrehajtása során a következő kérdéseket kell figyelembe venni:

- A mutatóknak mérhető információkat kell szolgáltatniuk (százalékok, átlagok és számok).
- A mutatókat támogató adatoknak könnyen beszerezhetőknek kell lenniük.
- A méréshez csak megismételhető folyamatokat kell figyelembe venni.
- A mutatóknak hasznosnak kell lenniük a teljesítmény nyomon követése és az erőforrások irányítása szempontjából.

A szervezeten belüli biztonsági metrikák programjának négy egymástól függő összetevőt kell tartalmaznia (lásd 7. számú ábra).



8. ábra: Információbiztonsági biztonsági metrikák, forrás: NIST Special Publication 800-55, biztonsági mérési programstruktúra

A 8. számú ábrán az látható, hogy mindennek az alapja az erős felsővezetői támogatás, ennek hiányában nehezebb hatékonyan és eredményeket elérni. Erre épülhetnek az irányelvek és eljárások amelyek a napi munkafolyamatokban érvényesíthetőek. Szükséges olyan teljesítménymutatókat választani, amelyek lehetőség szerint automatizáltan feldolgozhatóak és kvantifikálhatóak, idősorosan összehasonlíthatóak. A fejlődéshez és visszacsatoláshoz szükséges annak kimutatása, hogy elértük-e a kitűzött eredményeket, vagy mely területeken van szükség még fejlesztésre. Ezeket az adatok, mérőszámok elemzéséből lehetséges megtenni. A biztonsági metrikáknak kimondva, vagy kimondatlanul, de vissza kell köszönnie a biztonsági progtamban a hatékonyság érdekében.

Az erős felső szintű menedzsmenttámogatás megalapozása kritikus fontosságú nemcsak a biztonsági program sikeréhez, hanem a biztonsági metrikák programjának végrehajtásához is. Ez a támogatás a biztonságra összpontosít a szervezet legmagasabb szintjén. Szilárd alap nélkül

(vagyis az informatikai erőforrásokat ellenőrző pozícióban lévő személyek proaktív támogatása nélkül) a biztonsági metrikák programjának hatékonysága kudarcot vallhat, ha azt politikai és költségvetési korlátozások kényszerítik.

A hatékony biztonsági mérőprogram második alkotóeleme a gyakorlati biztonsági szabályzatok és eljárások, amelyeket a hatóság támogat a megfelelőség érvényesítéséhez. A gyakorlati biztonsági politikákat és eljárásokat úgy határozzuk meg, hogy azok elérhetőek legyenek, és megfelelő ellenőrzések révén értelmes biztonságot nyújtanak. A mutatókat nem könnyű megszerezni, ha nincs megfelelő eljárás.

A harmadik elem olyan mennyiségileg mérhető teljesítménymutatók kidolgozása és létrehozása, amelyek célja a lényeges teljesítményadatok rögzítése és biztosítása. Jelentős adatok biztosítása érdekében a számszerűsíthető biztonsági mutatóknak az informatikai biztonsági teljesítménycélokon és célkitűzéseken kell alapulniuk, és könnyen elérhetőnek és mérhetőnek kell lenniük. Ismételhetőnek kell lenniük, releváns teljesítménytrendeket kell biztosítaniuk az idő múlásával, és hasznosnak kell lenniük a teljesítmény nyomon követése és az erőforrások irányítása szempontjából.

Végül magának a biztonsági mérőprogramnak hangsúlyoznia kell a metrikák adatainak következetes időszakos elemzését. Ezen elemzés eredményeit felhasználják a megtanult tapasztalatok alkalmazására, a meglévő biztonsági ellenőrzések hatékonyságának javítására és a jövőbeli ellenőrzések tervezésére, hogy azok megfeleljenek az új biztonsági követelményeknek. A pontos adatgyűjtésnek prioritást kell élveznie az érdekelt felek és a felhasználók részéről, ha az összegyűjtött adatoknak jelentőségük van az általános biztonsági program irányításában és fejlesztésében. (NIST 800-55)

Az informatikai biztonsági mutatók a szervezet különböző szintjein szerezhetők be. A rendszerszinten összegyűjtött részletes mutatók összevonhatók (aggregálhatók) és felépíthetők egy fokozatosan magasabb szintre a szervezet méretétől és összetettségétől függően.

A siker csak akkor érhető el, ha a programot a meghatározott szervezeti felépítés, folyamatok figyelembevételével és az ésszerű erőforráskorlátokon belül szervezik meg és hajtják végre.

A metrikák fejlesztési folyamatának szakaszában a NIST 800-55 szerint a szervezeten belül bárki információbiztonsági érdekelt fél lehet, bár egyes funkciók nagyobb jelentőséggel bírnak, mint mások.

Az elsődleges informatikai biztonsági szereplők:

- A szervezet vezetője
- Információs vezérigazgató (CIO)
- Biztonságiprogram-menedzser / Információs rendszer biztonsági tisztviselő (ISSO)

- Programmenedzser / Rendszertulajdonos
- Rendszerbiztonsági tiszt
- Rendszergazda / hálózati rendszergazda
- IT-támogató személyzet

A másodlagos biztonsági érdekelt felek azon szervezeti egységek tagjai, amelyek elsődleges feladata nem a biztonság, ám működésük egyes szempontjai a biztonságot érintik.

Példák a másodlagos biztonsági érdekeltekre:

- Pénzügyi vezérigazgató (CFO)
- Képzési szervezet
- Humánerőforrás / személyzeti szervezet
- Általános ellenőrök (IG - Inspectors General)

Az egyes érdekelt felek érdekei különböznek, szerepük biztonsági szempontjaitól és a szervezeti hierarchián belüli helyzetüktől függően. Minden érdekelt félnek szüksége lehet egy további testreszabott mutatókészletre, amely áttekintést nyújt a szervezet informatikai biztonsági teljesítményéről a felelősségi körön belül. Az érdekelt felek érdekeit több helyszínen is meg lehet határozni, például interjúk, brainstorming-ülések és küldetési nyilatkozatok áttekintése révén. A mutatók száma összesen öt és tíz között legyen egy adott érdekelt fél számára. Javasoljuk, hogy érdekelt felenként kevesebb mutatót használjunk, amikor egy szervezet biztonsági programot állít fel; az érdekelt felekre eső mutatók száma fokozatosan növekszik az informatikai biztonsági program és a metrikák programjának lejártával.

Az érdekelt feleket be kell vonni a biztonsági mutatók fejlesztésének minden lépésébe, hogy biztosítsák a szervezeti bejutást a biztonsági teljesítmény mérésének koncepciójához (organizational buy-in to the concept). Az érdekelt felek bevonása azt is biztosítja, hogy a rendszerbiztonsági mutatók tulajdonosi érzése fennálljon a szervezet több szintjén, hogy ösztönözze a program általános sikerét.

Ugyanakkor fontos megemlíteni, hogy a mérés életciklusában a kiértékelésének és a megfelelő visszacsatolnak kiemelt jelentősége van. A visszacsatolásnak kell hoznia azokat az eredményeket, amelyek révén jó eséllyel az adott kockázat csökken, vagy amennyiben nem, egyéb megfontolásokat szükséges alkalmazni. Az egyéni szint mérése és látása azért fontos tehát, hogy ha elfogadjuk a leggyengébb láncszem elméletét, akkor láthatóvá váljanak a fejlesztendő területek.

Azt is fontosnak tartom megemlíteni, hogy a compliance distance, a megfelelőségi állapot változásának, a nemmegfelelőség megjelenésének, növekedésének, változásának mérésére az automatizált mérések nem minden esetben képesek, vagy pedig csak akkor, ha a trendek

idősorosan rendelkezésre állnak. Ilyen területekre sok esetben csak az interjúk vagy a szervezeti folyamatok pontos ismerete szolgálhat input adattal. A mérés és a nemmegfelelőségek megjelenésének észlelését disszertációmban részletesen compliance distance néven mutatom be. Ez úgy valósulhat meg, hogy a modellem alapján kidolgozott oktatások révén a felhasználók támogatottak abban, hogy visszajelzéseket adjanak az oktatott, bemutatott elvárásokról (szabályzat), az egyes egyének a saját folyamataikban érzékelt eltéréseket vissza tudják csatolni. Ezen visszajelzéseket csak akkor képes fogadni a szervezet, ha az oktatási folyamat során azt megtervezték, ilyen platform vagy lehetőség adott. Ennek hiányában a compliance distance észlelésében rejlő előny ezen területen belül nem kihasználható, a szervezet elvesztheti ezen visszajelzéseket, a nemmegfelelőségek megjelenését nem tudja érzékelni, mérni, vagy kisebb mértékben, elemszámban érkeznek adatok.

A mérés és kiértékelés kapcsán meg kell említeni, hogy számos nagyvállalat már alkalmaz valamilyen SIEM (Security Information and Event Management) rendszert. Ezek az automatizált rendszerek mindenképpen hasznosak az információbiztonsági szakterületen dolgozók számára. (Michelberger, Dombora, 2016) Az érzékelés és visszajelzés, valamint a kézi elemzés jelentős része automatizálható, így a hunting vagy egyéb mély szakmai területeken történő feladatok ellátására több idő allokálható. Ugyanakkor bár számos informatikai, információbiztonsági eseményre illeszthető szabály, a szabályalkotásra is erőforrásokat kell allokálni. Michelberger (2015) szerint is figyelembe véve, hogy "a leggyengébb láncszem az ember, a naplóelemzés egyik legfontosabb eleme a felhasználói tevékenységek elemzése, felhasználói profil kialakítása, ezek alapján a szokatlan tevékenységek azonosítása és elemzése." Azaz mind a SIEM, mind pedig a felhasználói aktivitás analízise (User and Event Behavior Analytics, UEBA), gyors feldolgozása és a preventív vagy reaktív reakció kulcsfontosságú (Michelberger, 2013) a megoldási folyamatok közé kategorizált az MSZ ISO/IEC 20000 és ITIL alapján. Mindezekre dolgozatom nem fókuszál, de a modern, automatizálásra törekvő információbiztonsági irányítási rendszer informatikai támogatása valóban elképzelhetetlen ezen rendszerek, automatizmusok nélkül, mindamellett Michelberger (2015) is hangsúlyozza az automatizmusok létrehozása során a felhasználói profilozás szükségességét.

3. A KUTATÁS ALANYAI ÉS A MÓDSZER

Ebben a fejezetben a kutatásomhoz felhasznált kérdőívekről, interjúkról, felmérésekről írok. Elsőként az interjúalanyokat mutatom be, ezt követően a felhasznált módszerek bemutatásával folytatom.

Számos oka van annak, hogy a szervezeteknek erőfeszítéseket kell tenniük és erőforrásokat kell megmozgatniuk az információbiztonsági tudatosság sikereinek értékelésére vagy mérésére. Posthumus és Von Solms (2004) indokolta az információbiztonság vállalatirányításba való beépítésének szükségességét, és keretet javasolt a szervezetek támogatására az integrációs erőfeszítéseik során. Az információbiztonsági tudatosságmérő eszköz fontossága tehát – a befektetés megtérülése, a biztonsági kampányok átirányítása stb. mellett – összekapcsolható a szervezet legmagasabb szintű vezetésével. Az információbiztonságnak jelentős szerepe van a menedzsmentfolyamatokban, így fontosak például az irányítási és az ellenőrzési szempontok. Ezek a szempontok egy szervezet vezetésének feladatai; feladataik ellátása érdekében megfelelő vállalati és információbiztonsági irányítási keretrendszerre van szükségük; valamint visszajelzésre arról, hogy mi történik a vállalatban az információbiztonság szempontjából. Mivel egy hatékony szervezet napjainkban nem képzelhető el informatikai támogatás nélkül, így az előbbihez, annak felhasználói és üzemeltetői számára megfelelő információbiztonsági szabályzat és szaktudás szükséges. Így rendkívül fontos, hogy elérjük az információbiztonság *alanyait*, megfelelő mintát tudjunk venni, és hogy az oktatás *módszerei* támogassák az átvinni kívánt tudást. Mindehhez a sikeres tudás és gyakorlat átadáshoz, amelynek része a mérés és visszacsatolás is, az általam bemutatott nemzetközi szakirodalom újszerű meglátást tesz hozzá, mivel kitűnik, hogy nem kizárólag magas szintű információbiztonsági szakmai, de további interdiszciplináris megközelítés is szükséges.

Meg kell említeni a nyomtatott anyagokra oly jellemző kitételt is disszertációm vonatkozásában, miszerint a mérés időpontja egy pillanatnyi lenyomatot rögzít. Ez egy dinamikusan változó állapot, így idővel természetszerűen változhat és változik is az információbiztonsági tudatosság állapota. Az adott mérés kiértékelése, feldolgozása és az arra való reagálás, ha ez nem automatizáltan történik, akkor akár jelentős időt vehet igénybe. Így az eredményekre való reagálás során a mérés óta eltelt időt is javasolt figyelembe venni.

További fontos tényező, hogy a kérdésfeltevéssel történő változtatás mértéke is, a "beavatkozás mérése". (Babbie 2001) "Nemcsak a program kimenetele szempontjából érdekes méréseket kell

elvégeznünk, hanem mérnünk kell a program szerinti beavatkozást: a kísérleti ingert is." (Babbie 2001) Ugyanakkor információbiztonsági oktatási szempontból kivétel talán a jelenállapot (baseline) mérés, vagy ha nem kutatási, kísérleti információk gyűjtése a cél, akkor mindenképpen üdvözölhető tény lehet akár a méréssel történő befolyásolás, oktatás. Tehát kijelenthető, hogy az információbiztonsági (egyéni és szervezeti) tudás egy dinamikusan változó állapot. Annak pontosságát befolyásolhatja a minta nagysága és a mintavétel csoportjának kiválasztása. Valamint "észre kell vennünk azonban, hogy egy mérőeszköz sűrűn használt volta önmagában nem biztosíték a megbízhatóságra." (Babbie 2001)

Általában véve a kutatásoknál jellemzően mintavételezésre van lehetőség. Ugyanakkor munkaszervezetek esetében, kötelező vizsgáztatásnál ennél sokkal pontosabb minta is rendelkezésre állhat. A kétféle mérési lehetőség közötti nagy különbség, hogy a nagy számok, a tömeg elfedhetik az egyéni kiugrásokat, devianciákat; míg a kismintás mérés esetén akár a csoportválasztás is döntően befolyásolhatja az eredményt. Tehát, amennyiben nem minden egyes elemről van információnk a teljes halmazban, akkor mintáról, mintavételről beszélhetünk, amely természetesen minden egyes mintában más lehet. Azaz általánosságban a nagy számosságra igazak lehetnek a megállapítások, de elképzelhető olyan csoport, szerepkör, vagy halmaz, amely az átlagtól jelentősen eltérő eredményt produkál. Mindez még jobban hangsúlyozza az oktatás és (mindenkire kiterjedő) mérés fontosságát.

Mindezeken kívül a "személyes érzelmek befolyásolhatják – és befolyásolják is – a kutatási kérdés megválasztását, a konkrét megfigyelések kiválasztását és a megfigyelésekből levont következtetéseket". (Babbie 2001) Azaz mind a válaszadó, mind a kiértékelő esetében is figyelembe veendő tényező a szubjektivitás.

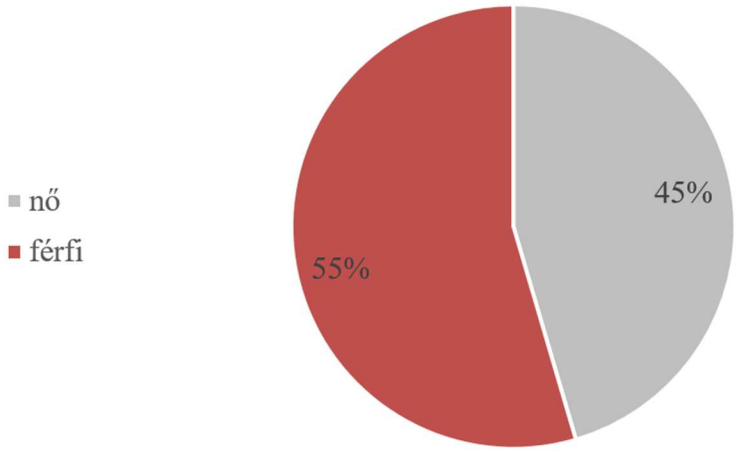
Végül "torzíthatja például a válaszokat a megrendelő rutinszerű megnevezése" (Babbie 2001) is, munkaszervezeti viszonylatban vizsgálva ez az információbiztonsági szervezeti egység megítélését jelentheti.

Mindezek figyelembevételével szükséges kezelni az eredményeket, amelyek jellemzően egy pillanatnyi állapotról adnak információt.

3.1. A KUTATÁS ALANYAI

3.1.1 ONLINE KÉRDŐÍV ALANYAI

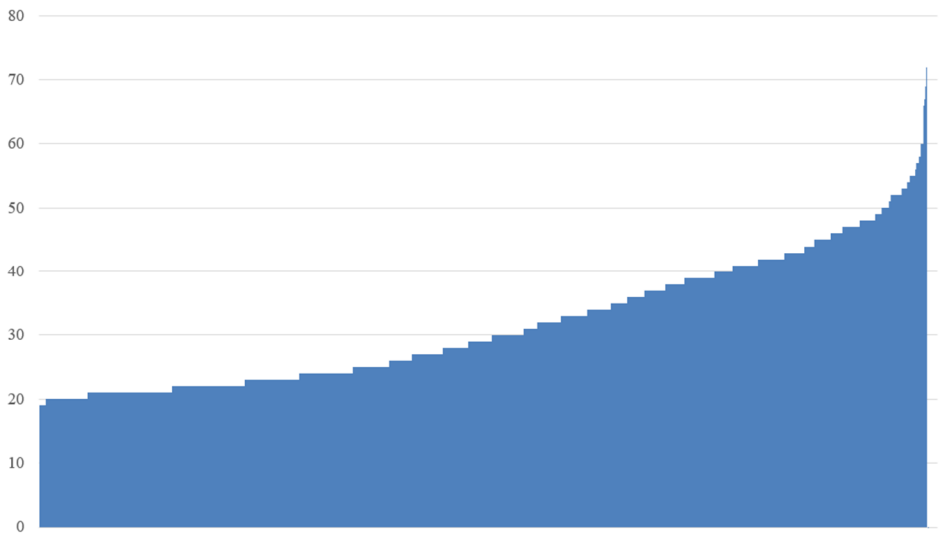
A 2013/14 fordulóján készített jelszóhasználati online kérdőíves felmérésemet összesen 1243 fő töltötte ki. Közöttük a nemek megoszlását a 8. számú ábra mutatja be.



9. ábra: Az online kérdőív kitöltőinek neme, eloszlása, forrás: saját szerkesztés

Az ábráról leolvasható, hogy a férfiak nagyobb számban (678 fő, azaz 54 százalék) töltötték ki a kérdőívet. Ez az eredmény meglepő, mivel általában a nők érzékenyebbek s empatikusabbak, s ők hajlandóak nagyobb számban egy-egy kérdőív kitöltésére. Az ábráról leolvasható, hogy a női válaszadók aránya 45% volt. Jelen esetben egy technikai kérdésről volt szó, ez magyarázatot adhat arra, hogy a nők kitöltési száma miért volt alacsonyabb. Azonban a közigazgatásban magasabb a nők aránya, és a kitöltők jelentős százaléka a közigazgatásból származik. Így összességében a mintán belüli eloszlás ezen okokra vezethető vissza.

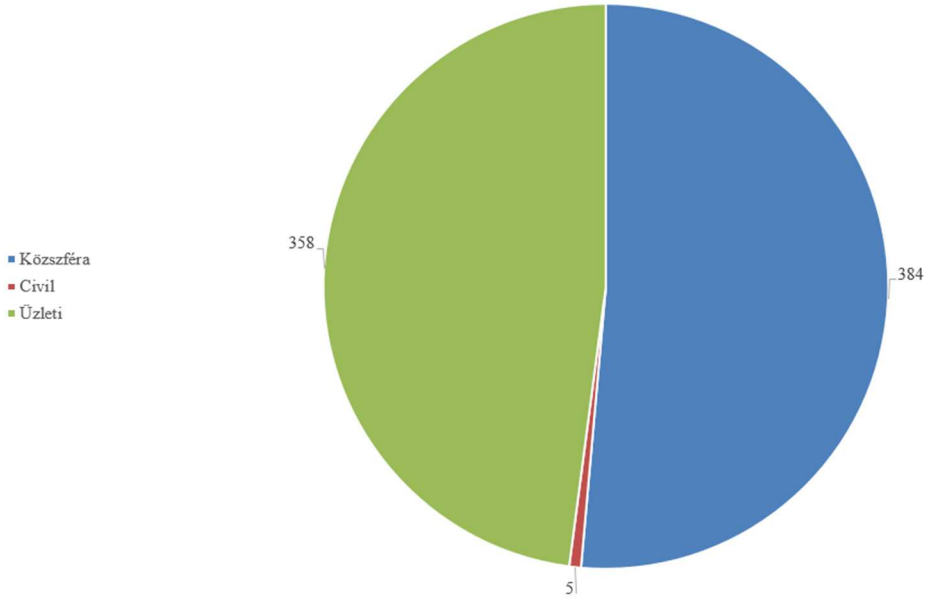
Ezt követően a kitöltők életkorát elemeztem (10. számú ábra).



10. ábra: Az online kérdőív kitöltőinek életkora, forrás: Saját szerkesztés

A 10. számú ábrán a függőleges tengelyen az életkor került feltüntetésre. Leolvasható az ábráról, hogy a legfiatalabb kitöltő 19 éves, míg a legidősebb 72 éves volt. Az átlagéletkor pedig 31,6 év. Ez alapján elmondható, hogy a kérdőív széles körben került kitöltésre, ami az életkort illeti.

A kitöltők között 747 fő volt aktív a munkaerőpiacon a kitöltése alapján. Három fő típust különítettem el a munkaerőpiaci besorolás szerint; kutatásomban a közszféra kerül a későbbiekben további alaposabb vizsgálat alá. A munkaerőpiaci eloszlás vizsgálatát az 10. számú ábrán teszem meg.



11. ábra: Az online kérdőív kitöltőinek eloszlása szféra szerint, forrás: saját szerkesztés

Az 11. számú ábrán vizuálisan megjelenítem a közszférában dolgozók számát. Ez 384 fő. Hasonló arányban kerültek ki a válaszadók, 358 kitöltő az üzleti szférát jelölte meg. A kutatás szakmai kiértékelése során ezt az adatsort, ezen kitöltői kört fogom további vizsgálatok alá vonni.

3.1.2. KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI KÉRDŐÍV ALANYAI

Az Illéssy, Nemeslaki, Som (2014) -kutatás során kíváncsiak voltunk a közigazgatásban dolgozók EIB-tudatosságának szintjére. Ez annál is fontosabb volt, mivel tudomásunk szerint eddig semmilyen szisztematikusan felépített adatgyűjtésből származó, empirikusan alátámasztott felmérés nem született még ebben a tárgyban Magyarországon. Ennek érdekében online kérdőívet tettünk ki a Nemzeti Közszolgálati Egyetem Tanulmányi és Vizsgaportáljára, amely a képzésben és továbbképzésben részesülő közigazgatási dolgozók számára egy kikerülhetetlen online felület.

A kérdőívet 379 fő töltötte ki, de az online kérdőívek egyik sajátosságának eredményeként minden kérdésre ennél kevesebben, 285-en válaszoltak.

A minta statisztikai értelemben nem reprezentatív, nem is lehet, hiszen a rendelkezésre álló szűk időkeret miatt erre nem volt lehetőségünk. A válaszokból kitűnik, hogy a kérdőívet kitöltők valamivel több mint fele (54%) nő, 46%-a férfi. Túlnyomó többségük (85%) budapesti lakos, a főiskolai vagy egyetemi végzettséggel rendelkezők aránya 90%. A válaszolók több mint kétharmada (68%) 45 évesnél fiatalabb volt, 32%-uk a 35 éves kort sem érte el. A 45-54 éves kor közöttiek aránya 23%, míg az 55 éves vagy annál idősebbeké 9% volt. Mindezek alapján tehát megállapítható, hogy a mintában valós súlyuknál feltehetően nagyobb arányban képviseltetik magukat a budapestiek és a fiatalok. (Illéssy, Nemeslaki, Som, 2014)

3.1.3 KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI INTERJÚK ALANYAI

A kutatás során a kvantitatív technikákat kiegészítettük kvalitatív módszerekkel, és 15 szakértői interjút készítettünk.

A kiszemelt és nyilatkozni hajlandó szakértőkkel félig strukturált mélyinterjúk készültek.

Természetesen ennyi interjúból nem lehet átfogó képet kapni a magyar közigazgatás rendszerében az információbiztonsággal kapcsolatban zajló folyamatok összességéről, ennek a kutatási technikának nem is ez a lényege. Nem is lehetett ilyen ambiciózus célunk a rendelkezésre álló szűk időkeret miatt sem. A kutatás azonban arra mindenképpen alkalmas volt, hogy azonosítsuk azokat a legfontosabb pozitív és negatív tendenciákat, melyek az elektronikus információbiztonság növelését célzó közigazgatási törekvéseket jellemzik, és amelyek hasznos útmutatóul szolgálhatnak az ehhez kapcsolódó képzések fejlesztésénél.

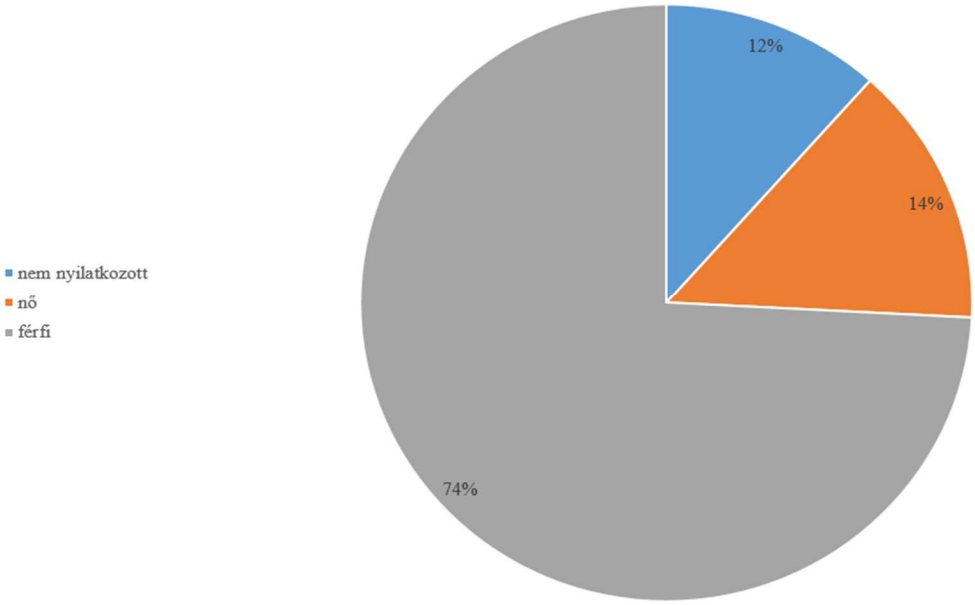
A 15 szakértői interjú alanyai közül 11 fő volt budapesti, 4 fő pedig vidéki telephelyen dolgozó munkavállaló. A nemek megoszlása szempontjából 4 fő nő, míg 11 fő férfi volt. A nemek és a vidék és város eloszlása nem esett egybe.

3.1.4 INFORMÁCIÓBIZTONSÁGI SZAKEMBER KÉRDŐÍV ALANYAI

A online kérdőív felmérése során 2014. 11. hó és 2019. 05. hó között került sor adatfelvételre. A felmérés során a Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzési szakon tanulmányokat folytató (leendő) információbiztonsági

vezetőknek biztosítottam lehetőséget a kitöltésre. Más, a képzésben részt nem vevő nem töltötte ki a felmérést. Összesen, adattisztítás után 155 kitöltéssel rendelkezett a kérdőív.

A kitöltésre anonim módon volt lehetőség. Demográfiai szempontból minden évfolyamon egyértelműen a férfiak voltak többségben, így a kérdőívet kitöltők között is ez jellemző: 115 férfi és 18 nő töltötte ki, valamint 22-en nem nyilatkoztak. Ezt vizuálisan a 12. számú ábrán mutatom be.



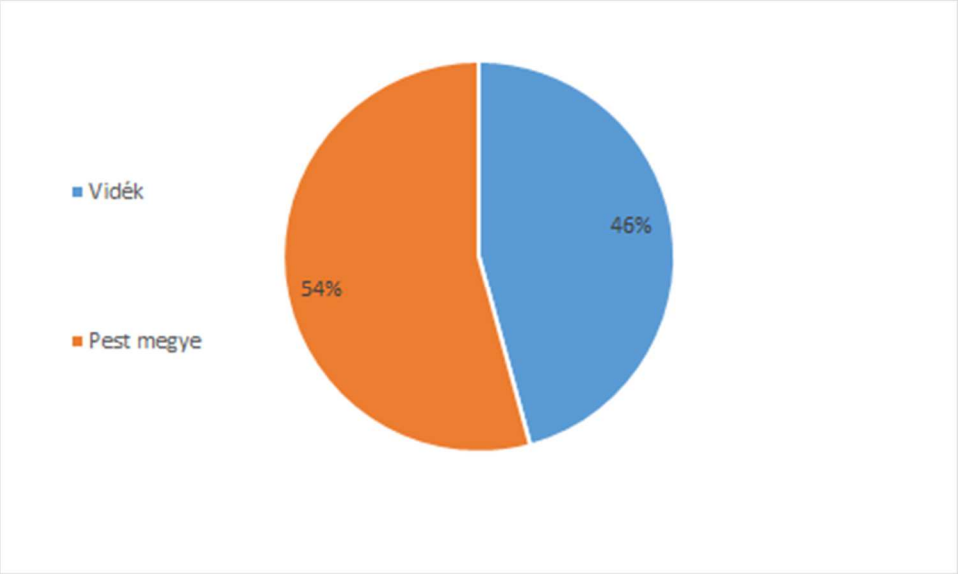
12. ábra: Információbiztonsági szakember kérdőív kitöltőinek nem szerinti eloszlása, forrás: saját szerkesztés

A 12. számú ábráról leolvasható a százalékos eloszlás is. A válaszadók 74%-a volt férfi, 14%-a pedig nő, valamint 12% nem nyilatkozott. A tipikus évfolyamlétszámokhoz viszonyítva ez rendkívül magas részvételi, illetve kitöltési arány.

A képzés bemeneti követelményei a Nemzeti Közszolgálati Egyetem weblapján is megtalálhatóak. Szakfelelős: Dr. Krasznay Csaba, egyetemi docens. A képzési idő 2 félév. A képzés óraszáma 280 óra. A felvétel feltétele: A képzésben legalább alapképzésben (korábban főiskolai szintű képzésben) szerzett oklevéllel rendelkezők közül vehetnek részt azok, akik angol nyelvű alapfokú komplex nyelvvizsgával vagy ezzel egyenértékű bizonyítvánnyal, oklevéllel rendelkeznek. A képzés fő célja "Az állami és önkormányzati szervek elektronikus információbiztonságáról szóló" 2013. évi L. törvényben meghatározott elektronikus információs rendszer biztonságáért felelős személyek feladatellátásához szükséges szakmai kompetenciák átadása és a biztonságtudatos szemléletmód kialakítása.

A képzés célcsoportja: A szakirányú végzettség birtokában az elektronikus információs rendszer biztonságáért felelős személy a megfelelő információbiztonsági rendszer kialakítása és fenntartása mellett ismereteivel és hozzáállásával növeli a szervezet biztonságát, neveli a munkatársakat, így összességében csökkenti a szervezet biztonsági kitettségét a hagyományos és informatikai támadókkal szemben. (Forrás: NKE EIV honlap)

Az egyes évfolyamok tekintetében egy 144 fős mintán vizsgálva a lakóhely[3] szerinti eloszlást, bár az első évfolyamokban elsősorban budapesti és Pest megyei[4] lakóhellyel rendelkező hallgatók voltak, ez később közel kiegyenlítődött, ahogy azt bemutatom a 13. számú ábrán.

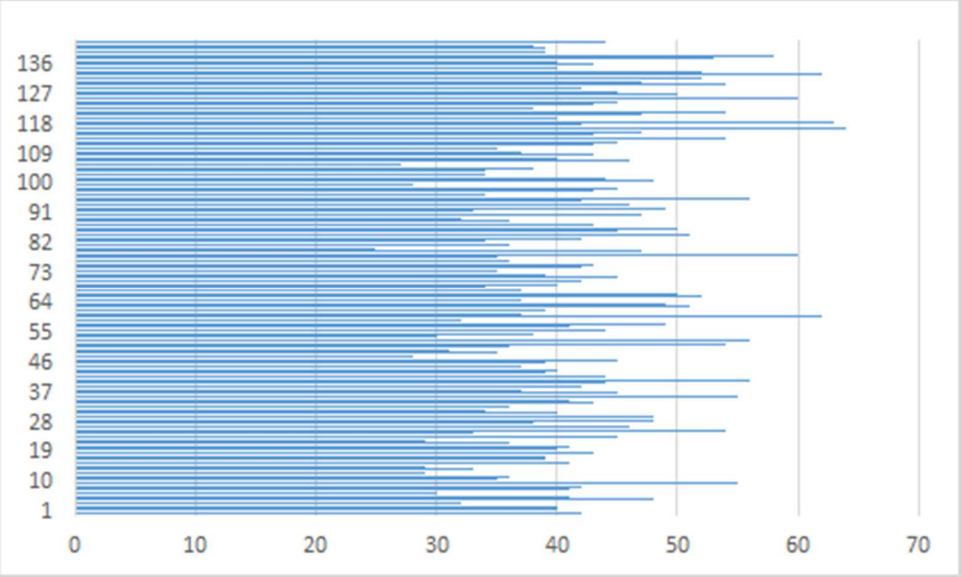


13. ábra: Információbiztonsági szakember kérdőív kitöltőinek geolokációs eloszlása, forrás: saját szerkesztés

A 13. számú ábráról leolvasható, hogy míg az első évfolyamokban többségében jelentős túlsúlyban voltak a budapesti vagy pesti lakóhellyel rendelkező hallgatók, addig ez az évek során szépen kiegyenlítődni látszik. A hallgatók 54%-a budapesti vagy Pest megyei bejelentett lakóhellyel rendelkezett, míg 46%-nak vidéki bejelentett lakóhelye volt az adatfelvétel időpontjában.

[3] A bejelentett állandó lakcím szerint.

[4] A vizsgálat fókusza a főváros és környékéről, ill. a vidékről érkező hallgatók aránya volt.



14. ábra: Információbiztonsági szakember kérdőív kitöltőinek életkor szerinti eloszlása, forrás: saját szerkesztés

Életkor szempontjából a kitöltők 25 és 64 év közöttiek voltak. Az átlagos életkor pedig 42,41 évre tehető. A 14. számú ábra függőleges tengelyén az egyes személyek jelennek meg, és a vízszintes tengelyen látható az egyes személyek életkora az adatfelvétel időpontjában. Így leolvasható, hogy 30 év alatti és 60 feletti hallgatók is részt vettek a képzésben. Tekintve a bemeneti feltételeket, azaz, hogy diplomával rendelkezni szükséges, logikus, hogy a legfiatalabb hallgató is 25 éves.

3.1.5 KÖZIGAZGATÁSI SZERVEZET TANTERMI INFORMÁCIÓBIZTONSÁGI KÉPZÉS ELŐTT/UTÁN KÉRDŐÍV ALANYAI

A kérdőív a 2013 őszén megtartott tantermi oktatások előtt és után került felvételre egy országos hatáskörű közigazgatási szervezet budapesti telephelyén.

A tantermi oktatás előtt (1 héttel) arra kértem e-mailben a résztvevőket, hogy töltsék ki az online kérdőívet. Az oktatás előtti kérdőívet 24 fő töltötte ki. Majd a tantermi oktatást követően pár nappal e-mailben ismét arra kértem a résztvevőket, hogy töltsenek ki egy másik, oktatás utáni kérdőívet. Az oktatás utáni kérdőívet 25 fő töltötte ki. A képzésen résztvevők aránya ⅓ nő és ⅔ férfi volt, ugyanakkor a kérdőívek anonim adatfelvétellel készültek, így a kitöltőkről további demográfiai információval nem rendelkezem.

3.1.6 "A" VÁLLALATI BEJELENTÉSI ESETSZÁMVIZSGÁLAT ALANYAI

Egy konkrét esettanulmány keretében egy vállalat adatait dolgozom fel, melynek nagyságrendileg 5000 alkalmazottja van. 2019. január 1-től állnak rendelkezésemre az informatikai és információbiztonsági bejelentések adatai. Ennek keretében e-mailen, valamint webes felületen és

telefonon tett felhasználói (hiba-) bejelentések kerültek összesítésre, feldolgozásra. A kutatás során első lépésként ezeket anonimizáltam, hogy a gyűjtött adatok feldolgozhatók legyenek.

3.1.7 "B" VÁLLALAT MUNKAVÁLLALÓINAK INFORMÁCIÓBIZTONSÁGI OKTATÁSA

2019-től hozzávetőlegesen 60 darab, részben tantermi, részben (a COVID miatt) online, Teams alkalmazáson keresztüli oktatás zajlott, összesen és nagyságrendileg 4500 fő részvételével.
Első lépésként a felsővezetői és középvezetői kör lett megszólítva, hozzávetőlegesen 330 fő, akiknek tisztán tantermi képzés került megrendezésre.
Ezt követően a második fázisban a közép- és alacsonyabb beosztású vezetőknek került meghirdetésre tantermi oktatás.
A teljes állomány részére szervezett képzés indulása pont egybeesett a COVID-szituációval, így számukra részlegenként 3 időpont-lehetőség került megadásra.
Az oktatásokon kötelező volt a részvétel, de arról videó készült, amelyet visszanézhetővé tettünk. A videót az oktatások végéig (hozzávetőlegesen 12 hónap alatt) összesen 1700-szor nézték vissza. Az oktatási videó terjedelme 1,5 óra volt.
Az oktatást követően vizsgát kellett tenni. Első körben részlegenként változó mértékű volt a vizsgán való részvételi arány, de 60% és 75% közé esett. Ezt követően az igazgatóságok vezetői emlékeztetőt kaptak a le nem vizsgázottak névsorával. Valamint a le nem vizsgázott személyek is emlékeztető e-mail kaptak. Így ezt követően egy héten belül 95% fölé emelkedett a vizsgázottak száma.

2019 decemberétől kezdtem meg a kidolgozott módszertan szerinti tantermi oktatás megszervezését, lebonyolítását és megtartását. Továbbiakban az "A" company vagy "A" vállalat vagy "B" company, "B" vállalat megnevezést alkalmazom. Elsőként az "A" munkaszervezet felső és középvezetése, nagyságrendileg 300 fő került kiválasztásra és meghívásra. A képzés tantermi oktatás formájában került kivitelezésre kiscsoportokban, azaz egy-egy oktatási időpontra maximum 40 fő került meghívásra, és az átlagos részvételi létszám 30 fő volt.

A második fázisban a közép- és további vezetők kerültek megszólításra, és szintén tantermi oktatás keretében ugyanebben az általam kidolgozott információbiztonsági módszertan szerinti oktatásban részesültek.

Harmadik fázisban az "A" vállalat minden munkavállalójára kiterjesztésre került a módszertan szerint oktatás. A kialakult vírushelyzet miatt válaszút elé kerültem, hiszen tantermi

oktatások megtartására nem volt lehetőség, és bizonytalan volt, hogyan és mikor lehetséges a megkezdett kutatást folytatni.

Ezért a módszertan szerint kidolgozott oktatás átdolgozása volt szükséges, hogy minden egyes meglévő modulblokk megtartásra kerüljön, de olyan módon, hogy online (és élő) Teams kooperációs platform alkalmazása mellett legyen lehetőség a részvételre. Az élő Teams-oktatásra való áttérés mellett a csoportlétszámot is megnöveltük, itt már 2-300 fő kapott meghívást egy-egy csoportba. Az átlagos részvétel 150-250 fő között mozgott. Egy-egy divíziónak átlagosan 3 alkalom került meghirdetésre, amelyek legalább egyikén kötelező volt a részvétel. Így a munkavállaló maga dönthetett a számára megfelelő időpontról. Az oktatás-sorozat végén további két pótidőpontot is meghirdettünk.

Az online (élő) oktatás során továbbra is fő fókuszban volt az interaktivitás, az önként jelentkezők bevonása stb. Az előadás a vezetői felelősségről és tennivalókról, valamint a kötelező vizsgáról szóló tájékoztatóval zárult. Az előadások közül az egyiket rögzítettük, hogy később visszanézhető legyen. Ez azóta az "A" vállalat intranetoldalán a legtöbbet visszanézett videó, több mint 1600-szor nézték vissza.

A kötelező vizsga (teszt) a Moodle rendszerben került rögzítésre. A teszt technikailag gyakorlótesztként lett definiálva, azaz akárhányszor megpróbálható, akár pontszámemelés céljából, akár sikertelen teljesítés esetén is, megengedve a többszöri kitöltési lehetőséget, míg klasszikus értelemben a vizsgatesztben ez csak egyszer lehetséges. Szakmai megfontolások alapján, a vizsgatesztet is az oktatási folyamat részeként kezelem, így minél többször ismétlik, annál jobb megértést, elmélyülést eredményezhet. Ennek megfelelően többszöri kitöltési lehetőség volt engedélyezve. Majd a kiértékelésnél lehet megvizsgálni, hogy ennek milyen számszerű eredményei vannak.

3.2. A KUTATÁS MÓDSZEREI

3.2.1. ÁLTALÁNOS KUTATÁSMÓDSZERTAN

A statisztika tudományán belül a mérési skála négy típusát különböztethetjük meg, melyek főbb jellemzőit Stevens (1946) foglalta össze.

Kehl (2011) cikkében összesíti a négy skálatípust, emellett kitér a méréselméleti vita történetére. Kiemeli Stevens azon megállapítását, hogy a mérésnek számos formája alapján különíthetők el mérési skálák – a négy alaptípus a nominális (névleges), az ordinális (sorrendi) és az intervallum (arány); és ezek a skálák határozzák meg a mérés során alkalmazott eljárásokat, valamint az adott

skála matematikai tulajdonságait. Ez lényegében azt jelenti, hogy az adott mérési skála meghatározza, hogy a meglévő empirikus adatok tekintetében milyen statisztikai módszereket, eljárásokat lehet és nem lehet alkalmazni.

A modern méréselmélet szerint, amely a skálák lehetséges típusainak matematikai meghatározásával foglalkozik, a Stevens által felállított négy skálatípuson kívül lényegében nem különíthetők el más jelentős struktúrák (skálák).

A mérési skálákat pár méréshez kötődő tulajdonságuk alapján kategorizálják – ezen a tulajdonságok a következők:

- Azonosság: A mérési skálán minden értékhez saját és egyedi jelentés köthető.
- Nagyság: A mérési skálán elhelyezkedő értékek sorrendi kapcsolatban állnak, egyes értékek nagyobbak, más értékek kisebbek.
- Egyenlő intervallumok: A skála egységeinek (pl. fokok) nagysága az egész skálán állandó.
- Nulla pont: Ha a skálának van tényleges nulla pontja, akkor annál kisebb értékek nem léteznek.

Ezen tulajdonságok alapján a következőképpen jellemezhető a négy alapvető skála:

- Nominális vagy névleges skála: Ez a skála inkább azonosít, kategorizálja a mérés tárgyát (pl. férfi / nő). Nagyságot nem tud meghatározni, mivel nem számszerűsít. Ez a skálatípus következésképp nem a legmegfelelőbb a szervezeti információbiztonsági tudatosság mérésére.
- Ordinális vagy sorrendi skála: Ezen a skálán megjelennek az azonosság és a nagyság kritériumai is. Minden értékhez egyedi jelentést társít, és ezek a skálaértékek sorba rendezhetők (pl. iskolai osztályzatok). Az érettségi modellek tipikusan ilyen skálát használnak, ezért a továbbiakban majd erre a skálatípusra fogunk fókuszálni.
- Intervallumskála: Az intervallumskálán az azonosság, a nagyság és az egyenlő intervallumok tulajdonságai is értelmezhetők. Ez a skálatípus az egyes értékek egymáshoz viszonyított nagyságát is mutatja, tehát hogy mely érték nagyobb, és hányszor nagyobb. Az érettségi modellek esetében ezt a tulajdonságot nem tudjuk értelmezni, mert annak a kérdésnek, hogy az „A” szervezetnél hányszor nagyobb az információbiztonsági tudatosság mint „B” szervezetnél, igazából nincs valós és értelmezhető jelentése.
- Arányskála: Az arányskálán a mérés mind a négy tulajdonsága értelmezhető – az azonosság, a nagyság, az egyenlő intervallumok fogalma is megjelenik, valamint létező nulla ponttal rendelkezik. Ez a mérési szint megint csak nem áll rendelkezésünkre ebben az esetben, amikor az információbiztonsági gyakorlat erősségét (az információbiztonsági

tudatosságot) szeretnénk értékelni egy szervezetben, hiszen nem tudunk egy abszolút zérus pontot mint kezdőpontot, megadni.

A négy alapvető skálatípusból tehát kizártunk kettőt (az intervallum- és az arányskálát), tehát az érettség mérésénél használt statisztikai eszközkészletet meghatározásánál a másik két skálatípusra kell koncentrálnunk.

A nominális vagy névleges skála a statisztikai elemzések során alkalmazott legalacsonyabb mérési szint. Itt adatokat sorolunk bizonyos kategóriákba (ahogy a skála elnevezése is mutatja), és nem követünk különösebb rendezési elvet vagy struktúrát. Egy igen/nem típusú skála például nominálisnak tekinthető – a kategóriák között nincs sorrendiség, távolságuk sem mérhető.

Az ordinális vagy sorrendi skála jobb mérési erősséggel bír. Ezen a skálán csak az abszolút sorrend jelenik meg, nem utal relatív távolságra. A legegyszerűbb formája a szimpla rangsor. Az ún. érettségi modellek ebből kifolyólag leginkább ezzel a típusú skálával dolgoznak. Ezen a szubjektív skálán az elhelyezett értékek közötti távolság nem tekinthető objektív távolságnak.

A mérés igazából valamilyen megfigyelésnek vagy automatizált adatmintavételnek a kvantifikálásából származik, hiszen az egyén, annak fizikai (SI) mértékegységbeli tulajdonságaitól eltekintve direktben nem mérhető. Azaz direkt, közvetlen módon nem lehet számszerű mérési eredményeket kinyerni valamely személy információbiztonsági tudatossági szintjéről. Ebből következik, hogy a személyek indirekt mérése és kvantifikálás után ez már a szervezetek, azaz embercsoportok esetében megvalósulhat.

Számos módszer lehet tehát az indirekt mérések lefolytatására és a kvantifikálásra, tehát (akár automatán) gyűjtött logok, naplóesemények által (viselkedési mintákat elemezve) vagy interjúkészítés révén, kérdőíves felmérés révén és ezek kiértékelése révén számszerű eredmények (kvantifikált értékek, számok) állhatnak rendelkezésre. Fontos ismét megemlítenem, hogy ezen értékek a jelenállapot mérésére szolgálnak, a változás önmagában korlátozottan, csak kontextusában értelmezhető. Ezen számok jelentését kontextusukban értelmezni kell tudni (sok, kevés, elfogadható, határértéken belüli stb.) További teendőként merül fel, hogy kommunikálni is kell tudni a számokat a vezetőség felé a cselekvési terv jóváhagyása miatt. A fókusz azonban a mérésen van: hogyan lehet mérni egy ember, a tudását, különösen azt, hogy ezt a tudást adott helyzetben mennyire akarja vagy mennyire tudja érvényesíteni, mennyire szabálykövető, vagy éppen a tudás hiánya miatt nem tudja követni a szabályzatokat. Ahhoz, hogy a mérés ne csak egy pillanatfelvétel legyen, kontextusba és idősoros elrendezésbe is kell illeszteni. Tehát az egy- vagy többféle méréssel felvett és kiértékelt adatainkat, ha mérünk valamit, akkor meg is kell(ene) tudni ismételni ugyanolyan vagy másféle módszertannal annak érdekében, hogy a tervezett változást, az elmozdulást látni lehessen a meghatározott időtáv tükrében is. Végül, soha ne felejtsük el, sok

esetben a mérés befolyásolhatja a mérendő személyt vagy az eredményt is, illetve a következő mérésre adott eredményeket is, így javasolt kontrollcsoportok alkalmazása, ha tudományos igényességű és nem csupán adott munkaszervezetre érvényes értékeket kívánunk létrehozni.

A disszertációmban bemutatott kutatásaim során továbbá nagy hasznát vettem és sor került a doktori iskolában tanultak érdemi hasznosítására, témavezetői, oktatói konzultációkra. Támogatta és elmélyítette ismereteimet a műhelyvitákon, tudományos védéseken való részvétel, szakmai konferenciák feldolgozása, az egyes szervezeteknél elérhető, publikus információk áttekintése. Valamint a konzultáció a témában érintett szervezetekkel, nemzetközi információk begyűjtése, analízisekre és szintézisekre épülő következtetések levonása.

3.2.2. ONLINE KÉRDŐÍV MÓDSZEREI

A statisztikai adatfeldolgozás egyik fontos kezdeti lépése volt a kutatási munka céljának megfogalmazása és a cél eléréséhez szükséges terv, kérdéslista elkészítése. A tervezéskor a célból indultam ki, és a feldolgozás lépéseit a célból levezetve tulajdonképpen visszafelé terveztem meg. A cél, mind a hipotézis, mind pedig a jelszóhasználati szokások mint indikátor felhasználásának viszonylag pontos megfogalmazása után meghatároztam a közlés (kérdésfeltevés) és az elemzés módját. Ennek alapján elkészítettem a kérdőívet és adatfeldolgozási tervet. Ezután a felmért szükséges adatok begyűjtése, a kérdőívek kitöltése, az adatfelvétel tervezése és megvalósítása következett. Végül a szükséges szervezési teendőkre tértem át. Azaz a kérdőívek kiküldése jelentős szervezést igényelt, valamint mivel geolokáció szerint elkülönítettem a kérdőíveket, így nyomon tudtam követni, hogy alacsony kitöltöttség esetén kit szükséges megszólítanom. Az adatfelvételt az adatfeldolgozás, az elemzés és értékelés és végül az eredmények közlése követte. A statisztikai adatok tisztítása, az adattisztítás az adatfeldolgozás egyik bevezető lépése. Az adattisztítás során felmértem a felvett adatokban rejlő (lehetséges) hibákat. Ez az adatfájl szerkezeti épségére, a hiányzó értékekre, az adatközlési és az adatbeviteli hibákra is kiterjedt. Az egyszerűbb és szembetűnőbb hibalehetőségek ellenőrzésén túl megvizsgáltam az egyes változók eloszlását is: az eloszlások szélein elhelyezkedő extrém értékeket vagy konstans alacsony vagy magas értékeket, illetve ilyenkor szükséges felmérni, hogy az eloszlások megfelelnek-e az előzetes elvárásainknak. Ha szükséges, akkor a kérdőív, a kérdések pontosítása is szükséges lehet. Kérdés még, hogy a változók letárolását megfelelően végezte-e el a rendszer.

Az online kérdőív összeállítása során 3 nagy blokkot alkalmaztam: demográfiai kérdések, információbiztonsági kérdések és IKT (informatikai jártassággal) összefüggő kérdések.

A kérdőív 2. számú mellékletben található.

Az egyes elemszámok szerint:

1.1 - 1.8: demográfiai kérdések

2.1 - 2.52: információbiztonsági kérdések

3.1 - 3.12 IKT (informatikai jártasság kapcsolatos) kérdések

A válaszok vizsgálata során számos statisztikai összefüggést vizsgáltam, ezek rövid bemutatása következik. Kolmogorov-Smirnov próba egy statisztikai teszt, ami a nem-paraméteres próbák közé tartozik. A teszt két minta eloszlásának összehasonlítására alkalmas. Egymintás t-próbát vizsgálunk vele a tapasztalati és az elméleti eloszlásfüggvény eltérésének maximuma alapján. Alkalmas arra, hogy két valószínűségi változó eloszlását összehasonlítsuk, vagy ellenőrizzük, hogy egy valószínűségi változónak csakugyan az az eloszlása, amit feltételeztünk. A próbát Andrej Nyikolajevics Kolmogorov dolgozta ki. Előnye, hogy eloszlásfüggetlen, és nem csak normális eloszlásból származó statisztikák vizsgálatára alkalmas, valamint a khi-négyzet próbával szemben kis elemszámú minták vizsgálatára is használható. (Bolla, 2005)

A próba szignifikáns jelentése: A statisztikai hipotézisvizsgálatban egy eredmény akkor mondható statisztikailag szignifikánsnak, ha ez a nullhipotézis mellett nagyon valószínűtlen lenne. Vagyis egy feltételezés előre meghatározott szignifikanciaszintje (jele: α) annak a valószínűsége, hogy a tanulmány elutasítja a nullhipotézist, azt feltételezve, hogy az igaz. Az eredmény p-értéke: (p) annak a valószínűsége, hogy (legalább) egy kiugró eredményt kapjunk, ugyancsak azt feltételezve, hogy a nullhipotézis igaz. Az eredmény akkor statisztikailag szignifikáns a feltételek mellett, ha $p \leq \alpha$. Egy tanulmány szignifikanciaszintjét általában az adatgyűjtés előtt határozzák meg, és általában 5%-ra vagy ennél sokkal alacsonyabbra teszik, tudományterülettől függően.

A statisztikai szignifikancia kulcsszerepet játszik a statisztikai hipotézisvizsgálatokban, mivel ezt használják annak a meghatározására, hogy a nullhipotézis elutasításra kerül-e vagy sem. A nullhipotézis az alapvető feltételezés, miszerint semmi sem történt vagy változott. Ahhoz, hogy a nullhipotézist elutasítsuk, a megfigyelt eredménynek statisztikailag szignifikánsnak kell lennie, vagyis a megfigyelt p-értéknek kisebbnek kell lennie, mint az előre meghatározott α szignifikanciaszint.

Ahhoz, hogy megállapítható legyen egy eredményről, hogy az statisztikailag szignifikáns-e, ki kell számolni a p-értéket, ami annak a valószínűsége, hogy ugyanolyan vagy még nagyobb mértékű hatás mérhető, azt feltételezve, hogy a nullhipotézis igaz. A nullhipotézis akkor kerül elutasításra, ha a p-érték kisebb (vagy egyenlő), mint az előre meghatározott α-szint. Az α egyben

annak a valószínűsége is, hogy a nullhipotézis elutasításra kerül, miközben az valójában igaz (elsőfajú hiba). Általában 5%-nál vagy az alatt húzzák meg.

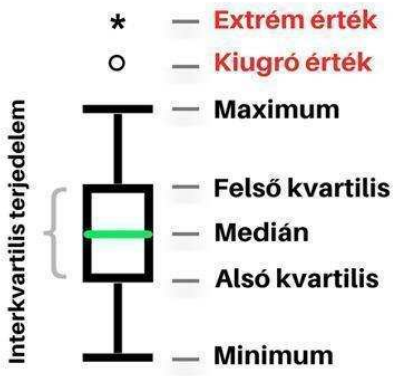
Mann-Whitney Test voltaképpen két független minta mediánegyezésének igazolására való eljárás. A nullhipotézis, hogy feltesszük, a két sokaság ugyanabba az eloszlásba tartozik. Gyakorlatilag a kétmintás t-teszt nem paraméteres megfelelője. Használatát a nem normál eloszlás indokolja.

Az interkvartilis terjedelem, a szóródás gyakori mérőszáma. Azt fejezi ki, hogy a rangsorban a középső 50%-ot lefedő elem mekkora intervallumban szóródik. A kvartilis eltérés a mediantól való átlagos eltérés. A boxplot diagram vagy más néven doboz ábra (Fogarassyné, Starkné, 2011) a változók eseteinek elhelyezkedését szemlélteti. Az interkvartilis terjedelmet egy dobozzal szemlélteti, amelyről leolvasható a medián és a kvartilisek. A legnagyobb és a legkisebb értékek egy-egy talppal vannak ábrázolva. Voltaképpen ez egy grafikus adatösszegzési módszer, amely vizualizálja és jobban érthetővé teszi a számszerű adatokat. (SPSSabc alapján, https://spssabc.hu/diagram-keszitese/doboz-abra) A doboz elhelyezkedése a teljes talphoz viszonyítva, illetve a medián helyzete a dobozon belül pedig információt ad az eloszlásról.

A doboz ábra további jellemzői, hogy egyes adatokat nem mutat, de mégis nagyon tömör, informatív. A doboz ábra kétféle kiugró adatot jelenít meg:

1. enyhén kiugró értékek, amelyek a belső határoló ponton kívül esnek, de a külső határoló ponton belül helyezkednek el, kör szimbólummal vannak jelölve
2. extrém kiugró értékek – a külső határolóponton kívüli értékek csillag szimbólummal vannak jelölve

A szimbólumok mellett az eset azonosítója (sorszáma) is megjelenik, így lehetőség van ezek visszakeresésére.



15. ábra: Doboz ábra értelmezése, Forrás: https://spssabc.hu/diagram-keszitese/doboz-abra/

A Chi-Square Tests, khi-négyzet próba két minőségi változó közötti kapcsolat elemzésére alkalmazható statisztikai próba. Vagyis arra ad választ, hogy a két változó között van-e szignifikáns kapcsolat. (Forrás: https://spssabc.hu/ketvaltozos-elemzes/khi-negyzet-proba/)

3.2.3 KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI KÉRDŐÍV MÓDSZEREI

A kérdőív kidolgozásánál az úgynevezett Security Awareness Survey (SANS) kérdőívét használtuk mintának, mert igyekeztünk a lehető legegyszerűbb és legrövidebb kérdéssort összeállítani Illéssy és Nemeslaki kutatótársaimmal. (Illéssy, Nemeslaki, Som, 2014) A SANS kérdőívét az USA-ban dolgozó információbiztonsági szakértők dolgozták ki; a hétköznapi felhasználói szokásokat méri fel, és azokhoz rendel 1-5-ig terjedő skálán egy értéket, majd az összesített értékek alapján öt kockázati kategóriába sorolja a válaszadókat.
A legalacsonyabb kockázati kategóriába tartozó munkavállalók jellemzője, hogy tisztában vannak a biztonsági alapelvekkel és veszélyekkel, jól képzettek, mindennapi viselkedésük megfelel a munkahelyi biztonsági sztenderdeknek és policyknak. A második legkisebb kockázatot jelentő csoportba tartozó munkavállalók már vettek részt valamilyen IB-képzésen, tisztában vannak a veszélyekkel, de mégsem követik teljes mértékben a vonatkozó biztonsági alapelveket és sztenderdeket. Az átlagos veszélyt jelentő kockázati csoportba azok a munkavállalók tartoznak, akik tisztában vannak a veszélyekkel, és tudják, hogy bizonyos biztonsági alapelveket be kellene tartaniuk, de továbbképzésre szorulnak a témában. Esetükben különösen az jelent veszélyforrást, hogy nem ismerik fel biztosan az incidenseket,és nem tudják, mi a teendő ilyen esetben. A jelentős kockázati tényezőt jelentő csoportba tartozók nincsenek tisztában a biztonsági alapelvekkel és veszélyekkel, sem pedig munkaszervezetük biztonsági szabályzatával. A kimondottan magas kockázati tényezőt jelentő csoportba tartozó munkavállalók nincsenek tisztában a veszélyekkel, és nincsenek tekintettel a biztonsági szabályzatokra sem. Tevékenységük folytán a munkahelyi informatikai rendszer könnyen támadhatóvá válik a külső behatolókkal szemben. (Illéssy, Nemeslaki, Som, 2014)

A kérdőív 25 kérdésből állt, amelyek a következő nagyobb témákat érintették: munkaszervezet és szabályozás (7 kérdés), elektronikus információbiztonsággal kapcsolatos tudások és ismeretek mindennapi felhasználói környezetben (8 kérdés), informatikai eszközök használata és adatkezelés (3 kérdés), általános számítógéphasználati szokások, különös tekintettel a jelszavak kezelésére (7 kérdés). A kérdőív teljes terjedelmében megtalálható az 1. számú

mellékletben. A beérkezett válaszokat az SPSS statisztikai programcsomag segítségével dolgoztuk fel; a legfontosabb eredményeket teszem itt közzé.

3.2.4 KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI INTERJÚK MÓDSZEREI

Az Illéssy, Nemeslaki, Som (2014) kutatás során elvégzett 15 interjú során, mely interjúk többségét én készítettem el, két nagyobb kérdéscsoportra kerestünk válaszokat: milyen igényeket és elvárásokat támasztanak alanyaink a továbbképzésekkel kapcsolatban, illetve mi jellemzi az IB-felelősök kijelölésének közigazgatási folyamatát. Ennek érdekében nem csak azok véleményére és tudására voltunk kíváncsiak, akik központi szerepet játszanak és játszottak az IB-vel (információbiztonsággal) kapcsolatos kormányzati programok kidolgozásában és végrehajtásában, hanem arra is válaszokat kerestünk, hogy mindebből mi és hogyan szivárog le a „végeken", vagyis a közigazgatás nem országos intézményeiben. Ezért a szakértői interjúkat két csoportra osztottuk, az első csoportba azok a szakértők kerültek, akik kisebb vagy nagyobb befolyással bírnak az IB fejlesztését célzó országos politikák kialakítására, ezeket neveztük úgynevezett „szakértői interjúknak". A másik csoportba azok kerültek, akik ilyen befolyással nem rendelkeznek, viszont van rálátásuk arra, hogy milyen pozitív és negatív folyamatok kísérik például a törvény végrehajtását. Ezeket a típusú interjúkat úgynevezett „felhasználói interjúknak" neveztük el. A kutatás során elvégzett interjúk fontosabb adatait a következő, 3. sz. táblázat mutatja be.

Szervezet típusa	Interjúalany beosztása	Interjúkészítés ideje	Interjú típusa
Minisztérium	IB-felelős	2014. 01. 13.	Szakértői
Egyetem	IB-szakértő	2014. 01. 15	Szakértői
Egyetem	IB-szakértő	2014. 01. 16.	Szakértői
Országos hatóság	elnökhelyettes	2014. 01. 30.	Szakértői

Minisztériumi háttérintézmény	IB-szakértő	2014. 01. 31.	Szakértői
Informatikai szolgáltató	IB-igazgató	2014. 02. 05.	Szakértői
Informatikai szolgáltató	IB-szakértő	2014. 02. 05.	Szakértői
Informatikai szolgáltató	IB-szakértő	2014. 02. 05.	Szakértői
Minisztériumi szervezet	informatikai főosztályvezető	2014. 02. 06.	Szakértői
Országos IB-szerv	képzési felelős	2014. 02. 25.	Szakértői
Vidéki kisváros önkormányzata	HR-szakértő	2014. 01. 30.	Felhasználói
Vidéki kisváros önkormányzata	informatikus	2014. 01. 30.	Felhasználói
Vidéki nagyváros bírósága	informatikai osztályvezető-helyettes	2014. 01. 31.	Felhasználói
Megyei adóigazgatóság	humánigazgatási főreferens	2014. 01. 31.	Felhasználói
Vidéki nagyváros bírósága	IB-szakértő	2014. 02. 04.	Felhasználói

2. táblázat: Közigazgatási információbiztonsági szakértői interjúalanyok, Forrás: Illéssy, Nemeslaki, Som (2014)

Az ábráról leolvasható, hogy egyrészt rendkívül kevés időnk volt a szervezésre és lebonyolításra. Másrészt területileg is országos hatókörben kellett mozogni, így az utazásokra is jelentős időt kalkulálva, voltaképpen egy-egy interjúra jellemzően egy egész napot kellett számolni. Külön

nehézség volt tehát, hogy rövid intervallumon belül az interjúalanyoknak is megfelelő időpontot találjunk.

Látható, hogy a 15 interjúalany közel kétharmada a szakértői csoportból, a kicsit több mint egyharmaduk a felhasználói csoportból került ki. A felhasználói csoport kevésbé kompetens a képzés tartalmával kapcsolatban megfogalmazott szakértői és munkáltatói véleményekkel kapcsolatban – s mivel a kutatás célja ezen kérdés feltárása volt, az arányokat tudatosan alakítottuk úgy, hogy a szakértői csoport képviselői legyenek többségben. Az általánosan is igaz, hogy az alsóbb közigazgatási szinteken nagyobb a bizonytalanság, kevesebb a rálátás. Ez nem jelent feltétlenül hátrányt, hiszen nagy volumenű kérdések esetében, mint amilyen az információbiztonság, rendszerint felülről jövő kezdeményezések által történik a kérdés beemelése és fontosságának hangsúlyozása – főképp bürokratikus rendszerek esetében. A kezdeti bizonytalanságot a képzések, az IB személyi struktúrájának kialakítása és folyamatos működése mérsékelni fogja.

A kutatás során a felkért és nyilatkozatott szakértőkkel félig strukturált mélyinterjúk készültek. Részben eltérő vezérfonal alapján haladtunk a szakértői és felhasználói csoporttal, de mindkét esetben három nagyobb területre koncentráltunk: 1. az információbiztonság kérdése a közigazgatásban, 2. a képzendők körének kiválasztási folyamata, 3. a képzés tartalmával összefüggő kérdésekre, véleményekre, elvárásokra. A szakértői csoporttal való beszélgetés országos vagy nemzetközi tendenciákat érintett, míg a felhasználói csoport esetében a már elindult folyamatokból származó tapasztalatok, illetve az országos szinten felmerülő igényektől esetleg eltérő helyi igények álltak középpontban.

3.2.5 INFORMÁCIÓBIZTONSÁGI SZAKEMBER KÉRDŐÍV MÓDSZEREI

A Nemzeti Közszolgálati Egyetem Elektronikus információbiztonsági vezető szakirányú továbbképzési szakon (NKE EIV) folytatott oktatói munkám mellett kutatási tevékenységet is végezve, az ott tanulmányokat folytató (leendő) információbiztonsági vezetőkkel jellemzően minden évben, a szak indulását követően (2013 és 2019 között) kitöltettem egy, főleg szabadszavas válaszokat kérő kérdőívet. A kérdéssort online bocsátottam rendelkezésükre, és online, órán kívül volt lehetőségük az adott félév végéig kitölteni. Az NKE EIV hallgatóktól azt kértem, hogy több (kifejezetten hosszabb) mondatos és ne egyszavas válaszokat adjanak.

3.2.6 KÖZIGAZGATÁSI KÉPZÉS ELŐTT/UTÁN KÉRDŐÍV MÓDSZEREI

A kérdőív módszereit tekintve ugyanazon típusú kérdéseket ölel fel, mint a korábban bemutatott online kérdőív, azaz tartalmazott nyílt végű válaszokat, előre megadott válasz kategóriájú kérdéseket, 10 fokú Likert-skála típusú válaszokat, valamint eldöntendő kérdéseket is. Ezen felmérés is online került kitöltésre, a kurzus résztvevői között előzetesen kiküldött e-mail, illetve a kurzus vége után kiküldött e-mail segítségével. A kitöltés önkéntes volt.
A kiértékelés során a válaszokat diagramokon és ábrákon jelenítettem meg, a szabadszavas válaszokat szófelhőben foglaltam össze.

3.2.7 "A" VÁLLALATI BEJELENTÉSI ESETSZÁMVIZSGÁLAT MÓDSZEREI

Három, bejelentésre rendelkezésre álló e-mail cím, valamint egy rendelkezésre álló webes felület, mindezek összesített adatai kerültek elemzésre 2017-től 2021-ig, amelyben 2019-től szerepelnek az oktatás hatásai, hiszen onnantól áll a cég rendelkezésére képzés.
Az elemzés módszereihez trendillesztést vettem figyelembe.
A bejelentéseket anonimizáltan dolgoztam fel.

3.2.8 "B" VÁLLALAT MUNKAVÁLLALÓINAK INFORMÁCIÓBIZTONSÁGI OKTATÁSA

A "B" vállalat esetében e-learning megoldással, nem kötelező módon került publikálásra információbiztonsági oktatás. Ennek kialakítása során vizsgáltam, hogy a modellem mely részei és hogyan alkalmazhatóak egy ilyen nem jelenléti oktatás kidolgozása során. A tervezés, kialakítás során tehát szempont volt, hogy ugyanazon, a kidolgozott modellem szerint történjen meg az e-learning kialakítása is. Törekedtem rá, hogy az e-learning tervezői rendszer nyújtotta lehetőségek kiaknázásra kerüljenek. Például, de nem kizárólag a kitöltő csak akkor tudott továbblépni, ha klikkelt, ha elolvasott minden elemet, amelyet kötelezőként jelöltünk meg a fejlesztés során. Törekedtem rá, hogy a szükséges mértékben grafikai elemek, látványos, releváns tartalmak, részösszefoglaló, a jelenállapot felmérése szolgáló, valamint tananyagközi kérdések is megjelenjenek az anyagban. A kulcsüzenetek "sulykolása" is megvalósult, grafikailag is kiemelésre kerültek, és ismétléssel jobban rögzültek. A tananyagközi kérdéseknek több célja is lehet, az egyik, hogy használhatók részösszefoglalóként vagy visszajelzésként,, valamint az előzőleg áttekintett anyaggal kapcsolatos tudás mérésére. Másrészt a következő tananyagrésszel kapcsolatos kérdés használható akár a meglévő tudásszint (az alaptudás) mérésére is.

Az e-learning kurzusok gyakori eleme a teszt vagy vizsga. Ebből lehetséges gyakorló vagy vizsgateszt is. Általánosan a gyakorló tesztben van megengedve a többszöri kitöltési lehetőség, míg klasszikus értelemben a vizsgatesztet csak egyszer lehetséges kitölteni. Szakmai megfontolások alapján, mivel a kurzusok is nem kötelezőek, azaz önként választhatóak voltak, a vizsgatesztet is az oktatási folyamat részeként kezeltem; így minél többször ismétlik, annál jobb megértést, elmélyülést eredményezhet. Ennek megfelelően többszöri kitöltési lehetőség volt engedélyezve. Majd a kiértékelésnél lehet megvizsgálni, hogy ennek milyen számszerű eredményei vannak.

A kérdések kiválasztása kétféle módon történhet: az oktató választja ki, vagy a rendszer véletlenszerűen választotta ki. Ebben az esetben nem minden kérdés fordul elő a tesztekben. Az eredményeken túl a Moodle képes statisztikai paramétereket is visszaadni. Ezen statisztikai adatok a pszichometria témakörébe tartoznak. A pszichometria a pszichológia és az oktatási mérések elméletével és technikáival foglalkozik. Méri a tudást és a személyes jellemzőket is. A mérés eszközei kérdőívek, tesztek.

A teszt kitöltésének jellemzői:

az alany egyszer tölti ki,

ugyanazon kérdéseket kapja meg (esetleg kevert sorrendben),

“átlagos” csoport,

“átlagos” kérdések.

Ilyenkor az eredmények eloszlása normális kell, hogy legyen. A normális eloszlás alatt minden véges szórású, független, azonos eloszlású valószínűségi változó sorozatot értünk, ha sűrűség függvénye a megadott feltételeknek megfelelő. Kicsit leegyszerűsítve a mérési eredmények sűrűséghisztogramját (oszlopdiagramját) ábrázolva, felrajzolva, arra ilyenkor általában jól illeszthető egy haranggörbe. Vagy más, továbbra is jelentősen egyszerűsített megfogalmazást alkalmazva az f sűrűségfüggvény mínusz végtelen és plusz végtelenbe vett integrálja: 1.

Homogén tanulói csoportok teszteredményei általában normális eloszlást követnek.

Ezeket az elért pont és az elérhető összes pontszám alapján számíthatjuk. Cél, hogy az eredmény 50-75% között legyen.

Median: matematikai értelemben a sorba rendezett adatok közül a középső, teszt szempontjából a hallgatók fele érte el az adott a pontszámot.

Módusz: a leggyakrabban előforduló mintaelem értéke.

Median: 100%, ha a próbálkozások legalább fele elérte a 100%-os pontszámot.

Szórás: az összpontszámok szóródása.

Pontszámeloszláshoz tartozó aszimmetria: csúcsosság.

Az adatsorok jellemzéséhez a középértékeken kívül fontos tudni, hogyan helyezkednek el ehhez viszonyítva az adatok.

Pontszámításhoz tartozó aszimmetria (ferdeség): normális eloszlású mintához képest aszimmetria 0: normális.

Pozitív: jobbra tolt, felkészült a hallgató, vagy könnyű a dolgozat.

Negatív: balra tolt, gyenge a hallgató, vagy nehéz a dolgozat, cél -1 és 0 közötti érték.

Pontszámeloszláshoz tartozó csúcsosság: a lapultság, csúcsosság, hogyan viszonyul a normál eloszláshoz, normál eloszlásnál: 0, cél 0-1 érték.

A görbe két oldalának meredekségére jellemző, hogy ha nagyon meredek a csúcs, akkor bizonyos értékek túl gyakran fordulnak elő.

Belső konzisztencia együtthatója: cronbach-alfa – a tesztkérdések koherenciájának mértéke. A teszt homogenitisát méri, a teszt két felének korrelációjával becsülhető.

Hibaarány: a pontszámok szóródásának oka – a különböző próbálkozások pontszámai eltérnek, vagy véletlen lehet az oka. Ezt utóbbinak a mértéke a hibaarány. A standard hiba az átlagtól való eltérést mutatja. A tesztszerkezet elemzése a kérdésre, adott kérdésekre vonatkozó statisztikát jelenti. Az eszközmutató, facilit index, az átlagos pontszám százalékban kifejezve, ami jelentését tekintve:

F: < 5 nagyon nehéz vagy rossz a kérdés

6-10 nagyon nehéz

11-20: nehéz

21-34: kicsit nehéz

35-64: átlagos

65-80 elég könnyű

81-89: könnyű

90-94: nagyon könnyű

95-100: kivételesen könnyű

Szórás: standard deviation, a válaszolók válaszainak szórását méri százalékban kifejezve, és ezzel azt is, hogy mennyire diszkriminatív, mennyire tud különbséget tenni a jó és kevésbé jó tanulók között.

Diszkriminációs index: a kérdésre adott pontszám és a teljes pontszám korrelációja %-ban kifejezve. Azt méri, mennyire különíthetőek el a kérdéssel a jobb és gyengén teljesítő diákok. A magasabb érték a jobb az adott kérdés esetén (a jobban teljesítők a teszt többi részén is jobban teljesítenek).

A diszkriminációs hatékonyság annak becslése, mennyire jó a diszkriminációs index a kérdés nehézségéhez képest. A nagyon könnyű vagy nagyon nehéz kérdések nem különböztetik meg a különböző képességű diákokat. Természetesen az az alapvető cél, hogy a különböző képességű diákokat meg tudjuk különböztetni. A legjobb megkülönböztetést 30-70%-os eszközmutató esetén kapjuk.

A kutatásomban bemutatott e-learning tananyagok egy nyílt forráskódú Moodle rendszerbe kerültek betöltésre. Mivel disszertációmban az e-learning megnevezést alkalmazom, így fontos kitérnem arra, hogy annak milyen lehetséges és alkalmazható funkciói kerültek alkalmazásra, és melyek nem. Az e-learning rendszerek alkalmazásához is szükséges előzetesen meglévő IKT-jártasság, így ennek felmérése és az alkalmazás támogatása mindenképp szükséges. (Bujdosó 2014) Az általam elvégzett kutatás során elkészített 3 e-learning modul esetében az általam kidolgozott modell került alkalmazásra. Ugyanakkor az e-learning keretrendszer által nyújtott vagy lehetséges beállítások közül a vizsgáztatás, a felhasználói visszajelzés és a központi modul, azaz az importált tananyag (SCORM) lejátszása került felhasználásra a magától értetődő alapvető funkciókon kívül, mint a felhasználók bejelentkeztetése, a navigáció biztosítása a tananyagban, melyeket a keretrendszerek általában tartalmaznak. Később további vizsgálat tárgya lehet, hogy egyéb, például a tutor funkciók (népszerűsít, kommunikál, motivál, szocializál, elősegít) (Cueste, 2010) nem kerültek beépítésre, ilyen plusz humán erőforrás nem került bevonásra. Azaz az alkalmazott e-learning keretrendszer mellett egyéb, jelentős humán erőforrás nem került bevonásra. Így bár a fejlesztés során alkalmazva lett az ADDIE (Analysis, Design, Development, Implementation, Evaluation) megfontolás, de nem volt biztosítva a tananyag betöltését követően tutor, vagy a meghirdetését követően extra kommunikáció a tananyagokhoz. Az e-learning rendszerek és bennük elérhető funkciók, például, de nem kizárólag a virtual tanterem, a hallgatók egymás közötti tartalommegosztási és kommunikációs lehetősége, jelvények adományozása, automatikus oklevélkiadás funkciója vagy egyéb kollaborációs lehetőségek, fórum, párbeszéd folytatására alkalmas terek, cross platform megoldások, mobil applikáció, BYOD, a tartalom (saját) eszközön való elérhetőségének biztosítása, házi vagy önálló feladatok kidolgozásának kiadása vagy lehetősége, felvett, előre rögzített vagy élő (tutor szerepkörre jellemző) videók vagy egyéb ajánlott tananyagok nem kerültek a rendszerbe.

Lehetséges jövőbeli kutatás tárgya lehet, hogy jelentősen több humán erőforrás bevonása mellett a tutor szerepkörök (Cornelius, Higgison, 2000) és lehetőségek kiaknázásával lehetséges-e elérni az élő oktatás eredményeit. Így disszertációmban, bár egy konkrét e-learning keretrendszer, a Moodle került alkalmazásra, de annak, illetve általában véve az e-learning rendszerek nem minden lehetséges funkciója került megvalósításra.

3.2.9 SZÓFELHŐ MÓDSZERTANA

McNaught, Lam (2010) szerint is a szófelhő hasznos kutatási eszköz lehet az oktatás vagy kutatás segítésére. Bizonyítják, hogy lehetővé teheti a kutatók számára, hogy gyorsan megjelenítsenek néhány általános mintát a szövegben. A vizualizáció lehetővé teszi, hogy megragadható legyen a szövegben a közös téma, és néha még a válaszkészletek közötti fő különbségek vagy egyezőségek is gyorsan felderíthetőek. Kutatási eszközként azonban a szófelhőknek vannak bizonyos korlátai, és nekünk jól kell ismernünk őket. Először is, mivel a frekvencia az eszköz egyik fontos szempontja, azt állítanánk, hogy a stratégia a legjobban működik olyan szöveg elemzésénél, amelyben az egyes alanyok nyers írásbeli válaszait lehet elemezni, nem pedig például a kutatók által összeállított második szintű összefoglalókat vagy jelentéseket. A szófelhők másik korlátja, hogy a szavakat a kontextuson kívül kapják el.

A szófelhők minden szót elemzési egységként kezelnek. Az adott szavak gyakori említése nem mindig elegendő információ ahhoz, hogy az adott szót érintő pontos állítás, vélemény megjeleníthető legyen. Természetesen az sem lehetséges, hogy a többszázas, vagy többezres mintában a felhasználókat visszakövetem, és kódokat alkalmazok az eredeti szövegre.

Ez a részben mechanikus szövegmanipuláció viszonylag gyors, ugyanakkor akár megtévesztő is lehet, mert elhanyagolja a szavak szemantikáját, valamint a szavakból álló kifejezéseket és mondatokat. Így a megoldás a szóalakok leegyszerűsített kezelése, és nem a tényleges jelentésük miatt, hanem a blokkokban, egységekben kezelhetőségük végett. És bár önálló kutatási eszközként én sem ajánlom, de az alábbiakban felvázolt stratégia kutatási eszközként rendkívül hasznos, és képes ráirányítani figyelmünket trendekre, jelenségekre, összefüggésekre.

A szófelhő készítése adott kutatási kérdésre, azon kérdésére adott válaszok kiértékelése azonban rendkívül sok utómunkát igényelt annak érdekében, hogy az egyes szavak számos ragozott alakja ne külön-külön szóként jelenjen meg a szófelhőben vagy elemzésben, hanem valamilyen halmazt, csoportot alkotva. Ide tartoznak még a ragozott alakokon kívül a helytelen helyesírással írt szavak, az ékezet nélküli karakterekkel írt szavak, rövidítések, valamint a kis- és nagybetűs különbözőségekből fakadó eltérések is. Ezen tisztítást elvégeztem, amelyre természetesen csak a teljes szöveg áttekintése után volt lehetőség. Ezt követően a kötőszavak és ragok, ékezetes karakterek cseréjére is sor került.

Ezután volt lehetőség egy speciális megoldással, az egyes karaktersorozatok növelésével, a szótövekig eljutva meghatározni ezek darabszámát és gyakoriságát. Ez a gyakoriság került

reprezentálásra – fontos, hogy a tartalmi kontextus figyelembevételével vizuálisan – a szófelhőábrákban.

Ezen folyamat eredményeképpen állhat elő egy-egy szófelhő, amelynél természetesen vizsgálni kell a szótövek mellett az esetleges tagadó mondatkapcsolatokat és a rokon értelmű szavakat is. (Például: oktatás, tanítás, képzés, awareness stb.)

Mindezek érdekében elvégzett lépések:

- a kutatási kérdésre adott válaszok tanulmányozása, tipizálható csoportok keresése,
- a válaszok teljes szöveges átalakításainak elvégzése, egységesítés
    - ékezetes karakterek lecserélése ékezet nélküliekre
    - nagybetűk lecserélése kisbetűkre
    - írásjelek, egyéb jelek eltávolítása
- minden szó külön sorba rendezése,
- ABC sorrendbe rendezés,
- az így kapott soronkénti állapot áttekintése, szógyakoriság kézi vizsgálata, szótőkeresés, nagyobb halmazok meghatározása,
- az azonosított nagyobb halmazokra, szótőre keresés,
- a keresési eredmények lejegyzetelése, ennek betöltése a vizuális megjelenítőbe,
- ellenőrzés, a megjelenítés finomhangolása.

4. EREDMÉNYEK

4.1. AZ ELSŐ HIPOTÉZIS VIZSGÁLATA (H1)

Feltevésem szerint H1: Az információbiztonsági tudatosság szintjének tekintetében a magyar közigazgatás területén nem tapasztalható lemaradás a magyar üzleti szférával összehasonlítva. Ezen tézisem vizsgálatához több kutatás eredményeiből a vonatkozó kérdéseket értékelem ki. Elsőként annak a kérdésnek a körüljárását végzem el, hogy miért is jó indikátor *a jelszó* az információbiztonság tudatossági szintjének jelzésére.

A jelszó mint kifejezés is többféle megoldás gyűjtőneveként használható. Jó jelszó igazából nem létezik, és tökéletes biztonság se. Így disszertációmban az egy- vagy többfaktoros azonosítást is beleértem az azonosítás és hitelesítést folyamatát végletesen leegyszerűsítve. Tehát bár a jelszó kifejezést használom, de alapvetően a hitelesítést megvalósító karaktersorozat vagy eszköz, valamint az adat bizalmasságát garantáló egyéb megoldás is ide sorolható, tehát akár a többfaktoros azonosítás egésze vagy valamely része is.
A jelszónak mint a bizalmasság egyik zálogának jósága csak más ismérveken keresztül értelmezhető vagy mérhető. Tehát nem a jelszó lehet jó vagy rossz, hanem azt lehetséges vizsgálni, hogy az adott környezet (összesített védelem), amelyben a jelszó (mint az azonosításra alkalmazott módszer) használatra kerül, mennyire támadható. Továbbá vizsgálható az is, hogy ezt a komponenst hogyan használják a munkaszervezetben. Azaz a körülmények összességében határozzák meg az azonosítás-hitelesítés (jelszó) jóságát, vagyis támadásokkal szembeni ellenálló-képességét. További kérdés az is, hogy ezen használatot (oktatást, szabályozást stb.) hogyan lehetséges megfigyelni, operacionalizálni, és a megfigyelési eredményeket hogyan lehet kvantifikálni (számszerűsíteni). Cikkemben egy lehetséges módszertant mutatok be, mely képes támogatni a biztonsági szint mérését egy azonosított indikátoron keresztül. Természetesen további indikátorok definiálása válhat szükségessé, valamint egyes indikátorok környezetének meghatározása is szükséges lehet az indikátoron keresztüli komplex (munkaszervezeti-nemzeti) méréshez. A monitoring, indikátorok alkalmazásával akár egyes munkaszervezetek, eltérő közigazgatási szervek biztonsági szintje is összehasonlíthatóvá válhat, valamint ugyanazon munkaszervezetek biztonsági szintjének változása is nyomon követhető lehet. A módszertan egységes alkalmazása és kiterjesztése alkalmas lehet geolokációs, időbeli, életkori, munkaszervezeti, demográfiai és egyéb sajátosságok feltérképezésére is. Hosszú távon a mérési

eredmények kiértékelése által az egyes szervezetek képessé válhatnak fejlesztési irányvonalakat (egyre precízebben) meghatározni, és a létrehozandó fejlesztési stratégia, valamint a közigazgatásban elérhető több millió munkavállaló révén pozitív hatással lehetnek a nemzeti információbiztonsági, kibertudatossági szintre is. A módszertan további előnye, hogy más indikátorokra is alkalmazhatóvá tehető. A Nemzeti Közszolgálati Egyetem által gondozott Elektronikus információbiztonsági vezetőképző szakon létrehozott szakmai műhelynek köszönhetően a már végzett hallgatók segítségével akár több száz a 2013. évi L. törvény által érintett közigazgatási szervezet válthat elérhetővé. A cikkben a teljes módszertanból két terület kerül bemutatásra. Ebből következnek megállapítások, amelyek alátámasztják, hogy akár a jelszó is képes lehet arra, hogy (egyik) indikátora legyen az információbiztonsági szintnek, támogassa a fejlesztések megtervezését. A jelszóhasználatra vonatkozó kutatásaim és a szakirodalmi áttekintés is azt támasztotta alá, hogy a jelszóhasználat megfelelő indikátor. Egyes kutatások azt is kimutatták – a jelszavak visszafejtése révén számszerűsítve –, hogy az alkalmazott jelszavakban milyen változás történik az oktatást követően. Egyetlen példát megemlítve a 2846 azonosítót vizsgálva a 24 óra alatt visszafejthető jelszavak aránya 98.8%-ról, 63.6%-ra csökkent, és a rövidebb időtáv alatt visszafejthető jelszavakban is jelentős csökkenés volt mérhető. (Eminagao, 2009)

Ki kívánom emelni, hogy a jelszó vagy általában véve az azonosító, az alkalmazott hitelesítési megoldás, mindezekkel kapcsolatos olyan tényező, amely kvantifikálható, alkalmas lehet az információbiztonsági szabálykövetési gyakorlat mérésére mint indikátor. Ez természetesen nem jelenti azt, hogy elegendő kizárólag ennek vizsgálata az információbiztonsági tudásszint nyomonkövetéséhez, értékeléséhez. Ugyanakkor mindenképpen szükséges lehet egyéb indikátorok alkalmazása is. Valamint "észre kell vennünk azonban, hogy egy mérőeszköz sűrűn használt volta önmagában nem biztosíték a megbízhatóságra." (Babbie, 2001) Azaz szükséges lehet időközönként az indikátorok újraértékelése, frissítése, cseréje abban az esetben is, ha egyébként megfelelő értékeket mutatnak.

Így szükséges olyan áttekintés és lehetséges mérési módszertan létrehozása és közreadása, mely által összehasonlíthatóvá, kiértékelhetővé válik a magyar közigazgatási szervezetekben a jelszóhasználati (azonosítási-hitelesítési megoldások használatával kapcsolatos) gyakorlat. Ennek révén a mérés, oktatás, mérés megismétlése, egyfajta PDCA modell alkalmazása, amely idősoros méréseken keresztül a gyakorlat fejlődését vonhatja maga után. A módszertan további indikátorokra való alkalmazásával alkalmassá tehető a közigazgatási információbiztonsági szint értékelésére, fejlesztésére. Az indikátorok kiválasztása és mérése által létrejövő idősoros eredmények nem kizárólag az adott szervezet információbiztonsági stratégiáját képesek

támogatni, hanem fejlesztésre, munkaszervezetek és egyéb fókuszpontok összehasonlítására is alkalmassá tehetők; ezen túlmenően előrejelzéseket is szolgáltathatnak.

Számos szakirodalom foglalkozik a jelszavak történelmével, kialakulásával, az első használt jelszavakkal, így cikkemben ezzel nem foglalkozom. Tény, hogy több száz, több ezer évre nyúlik vissza annak eredete. Az emberek mindig próbálták valamilyen módon megvédeni az információt. Ez a kor technikai fejlettségének függvényében folyamatosan változott.

Napjainkban, az elmúlt 50 évet tekintve talán az egyik legjelentősebb változás az információs rendszerek számítási kapacitásának ugrásszerű növekedése. Valamint, hogy a számítási kapacitás már széles körben (nem csak lokálisan) vált elérhetővé. Ezenkívül az információs rendszerek elterjedtsége mind a privát, mind a közigazgatási szektorban szintén jelentős. Mindezen alapvetések, melyeket axiómaként kezelek cikkemben, a későbbiekben hivatkozásra kerülnek.

A *jelszó* kifejezés alatt is sokkal inkább egy általános belépési (authentikációs) módszert kell értenünk napjainkban. Például nem kizárólag a klasszikus jelszó, hanem a PIN-kód, valamilyen (fizikai) kulcs alkalmazása, feloldó minta, biometrikus azonosítás stb. és ennek alkalmazása elektronikus vagy offline rendszeren is ide sorolható. Ennek az általánosításnak lényege, hogy egyrészt általánosítottam a jelszó fogalmát valamilyen védelmi mechanizmusra, másrészt pedig az adott védelmi megfontolás biztonsági szintjét annak környezete is (jelentősen) befolyásolhatja. Fontos megemlíteni, hogy bár egyszerűsítésként használjuk a hitelesítés-azonosításkor alkalmazott körülményekre a jelszó kifejezést, a technika fejlettségének, számítási kapacitásának függvényében folyamatosan változik a tipizálható támadási vektor; azaz napjainkban a többfaktoros azonosítások hasonló energiabefektetéssel, eszközökkel támadhatóak, mint pár évvel ezelőtt az egyfaktoros hitelesítés.

Jelenleg is léteznek már elszigetelt mérések az információbiztonságra egy-egy oktatást megelőzően, vagy azt követően annak megértésére, hatékonyságára a magyar közigazgatásban egyes munkaszervezetekben. Ezek azonban megfigyeléseim szerint lokális, szigetszerű mérések, egyes munkaszervezetekre korlátozódnak, időben nem ismétlődnek. A mérések struktúrája eltérő, így egyes az munkaszervezetekben végzett mérések nem összehasonlíthatóak. Ezen munkaszervezetekben a mérés jellemzően nem szabályzatból kiinduló tevékenység. Így szabályzat nélkül, felső szinten jóváhagyott és dokumentált kérdéslista nélkül a mérés évenkénti megismétlése, megismételhetősége esetlegessé válik. Azaz nem összehasonlíthatók, nem reprodukálhatók, nem megismételhetők ezen mérések.

Az a jelsorozat, amelyet az adott információs rendszer használatához megkövetelünk, számos egzaktul mérhető tulajdonsággal rendelkezik. Ilyenek lehetnek:

- hosszúsága,
- szekvenciális összetétele (kisbetűk, nagybetűk, számok, speciális karakterek)

- tartalmaz-e értelmes szót magyar nyelven
- tartalmaz-e értelmes szót valamely idegen nyelven
- újrafelhasznált-e (alma, alma1)
- életkora (az utolsó jelszó-változtatás időpontjától mért időbeli távolság)
- egyéb, további tényezők (Som, Papp, 2014)

Ezenkívül számos olyan tényező létezik, amely kevésbé egzakt módon mérhető, de jelentősen befolyásolja a „jelszó jóságát". A jelszó életciklusának szabályozottsága, matematikai visszafejthetősége és egyéb tényezők, összességében a körülmények és ellenálló-képesség is ide számíthatók.[5] [6] [7] [8] Mielőtt azonban ezen tényezőket katalogizáljuk, érdemes megvizsgálni a jelszó pontos funkcióját.

A jelszó alapvetően jelen cikk tárgyalási szempontjából az információbiztonsági szint egyik lehetséges indikátora, lehetőség annak mérésére. Belátható, hogy mindenkinek van valamilyen elképzelése a jó jelszóról, számos hazai és nemzetközi publikáció vizsgálja annak összetettségét, visszafejthetőségét, egyéb tényezőket. Azonban ha nem a „jelszó" szót használjuk, hanem a „megfelelő védelem" kifejezést, akkor a valósághoz kicsit közelebb kerülünk. Ez azt jelenti, hogy a valóságos cél az adott adat, információ, információs rendszer megfelelő védelme valamilyen „megfelelő védelem"-mel. Ez lehet a jelszó mint valamilyen karaktersorozat, lehet valamilyen jelszó és további birtoklásalapú komponens alkalmazása és lehet továbbá biometrikus kiegészítés alkalmazása is. Itt voltaképpen a három klasszikus a „tudok valamit", „van valamim" és „vagyok valami" azonosítás került felsorolásra.

Ezek után viszont már összegezhető, hogy a „megfelelő védelem" (jó jelszó) használata még abban az esetben is, ha „csak" a „tudok valamit" kategóriába esik, nem mérhető feltétlenül pontosan adott attributumokkal. A pontos valódi biztonsági szint megállapításához a környezetet (befolyásoló tényezőket) is javasolt figyelembe venni.

A jobb megértés érdekében mindezt példával kívánom illusztrálni.

Egy számítógépes hálózatról leválasztott, fizikailag és egyéb (például, de nem kizárólag irányított sugárzástól, lehallgatástól stb.) tényezőktől védett helyen lévő információs rendszer esetében akár megfelelő lehet (a kompenzációs kontrollok miatt) „rövid", párkarakteres jelszó használata is.

A nemzetközi kutatások és saját kutatásaim is azt támasztották alá, hogy a *kikényszerített, de nem támogatott* (meg nem értett) jelszóházirend (azaz a szabályozottság gyakorlattal való távolsága)

[5] The Tangled Web of Password Reuse, Anupam Das, Joseph Bonneau, Matthew Caesar, Nikita Borisov, and XiaoFeng Wang

[6] Effect of Grammar on Security of Long Passwords, Ashwini Rao, Birendra Jha, Gananand Kini

[7] The Security of Modern Password Expiration: An Algorithmic Framework and Empirical Analysis, Yinqian Zhang, Fabian Monrose, Michael K. Reiter

[8] How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation, Blase Ur, Patrick Gage Kelley, Saranga Komanduri, Joel Lee, Michael Maass, Michelle L. Mazurek, Timothy Passaro, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie Faith Cranor

csökkenti a „jelszó jóságát”. Azaz újrahasznált jelszavak keletkeznek (alma, alma1), vagy más módon törekednek az adott információs rendszer felhasználói a jelszavak memorizálására.
Mindezek alapján azt állítom, hogy a jelszóval kapcsolatban:

- számos tényező mérhető,
- számos tényező kvantifikálható, azaz mérhetővé és számszerűsíthetővé tehető.

Tehát összességében a teljes környezetet javasolt vizsgálni, mérni. Ennek a teljes információbiztonsági környezetnek és mindennek, ami erre hatással lehet – nevezzük univerzumnak – egyik lehetséges halmaza a jelszóhasználat. Ebből már következik, hogy további halmazok is léteznek. Ezen halmazoknak lehetnek metszeteik, de akár diszjunktak is lehetnek.
A jó jelszó azért nem értelmezhető, vagy legalábbis jelen állításban pontatlan fogalom, mivel az adott munkaszervezetre jellemző tipizálható támadási vektort (kockázatelemzést követően) kontrollintézkedések figyelembevételével lehetséges összességében kezelni és mérni.
Példaként említem az *adatlopás* kifejezést, amely szintén magyarázatra szorul (nem egyértelmű), mivel adatlopás esetén lehet, hogy adatszivárgásról van szó, amikor illetéktelen hozzáfér, lemásolja az adatokat. Valamint adatlopás lehet az is, amikor zsarolóvírussal titkosításra kerül az adat, és így válik hozzáférhetetlenné. Klasszikus értelemben a lopás alatt azt értjük, hogy valami elveszik, a hozzáférésünk megszűnik.
A „jó jelszó” mint megfelelő (kockázatarányos) védelem, a tipizálható támadási formák felmérését követően, azokra adott válaszként értelmezhető.
A jelszó elleni tipikus támadási formákra jelen cikkben csupán nagyon röviden kívánok kitérni. Két fő típusa van: az online, amikor valós időben (vagy visszajátszás révén, de még a session élettartama alatt) tudja a támadó megszerezni a tudást, vagy valamilyen módon visszaélni a megszerzett tudással; valamint az offline, amikor valamilyen rögzített adatbázis, vagy rögzített forgalom révén megfelelően nagy számítási kapacitással próbál a támadó értelmezni. Ezekre több száz, több (tíz)ezer különböző kifinomultságú, adott támadási formára specializálódott eszköz létezik (smart guesses, dictonary attack, brute-force attack, rainbow tables, social enginering, keylogger, sniffer stb.).

A támogatott információbiztonság végig kell, hogy kísérje az adott halmaz vagy azonosított biztonsági komponense teljes életútját. Ez nem csak a szabályzatokban, rendszerekben, oktatásban stb. kell, hogy megjelenjen, hanem összefüggő egészet képezve azonosítani kell kapcsolódásait. Tehát egy megfelelő erőforrás-kapacitással rendelkező információbiztonsági felelős meg kell, hogy értse az adott információs rendszert és annak minden olyan releváns munkafolyamatát, amely hatással lehet a biztonságra. Ezt természetesen iterálni

szükséges az adott szervezet online és offline rendszereire, valamint munkafolyamataira is – szolgáltatásként igény bevettekre is. A mérési lehetőségekre egy lehetséges (ellenőrző) lista létrehozásával láthatóvá válik, hogy miért szükséges a határterületek feltérképezése is.

A mérhetővé tétel érdekében összesen egy tucat terület került meghatározásra, melynek során felhasználásra kerültek a NIST 800-53 és NIST 800-63, valamint az MSZ ISO/IEC 27001:2014 szabványok. Ezen struktúrák tudásanyagát felhasználva készült, azonban elsődlegesen a tipizálható támadási vektor (a jelenleg ismert támadási formák) és az az elleni védelmi megfontolás szerinti struktúra alapján került kialakításra a kérdéssor. A mérés során figyelni kell a megfelelő tervezésre és a végrehajtásra. Például, mivel jellemzően nem lehetséges minden egyes munkavállalót a teljes kérdéslistával mérni, így a mintavételezést az egyes szerepkörökre, geolokációs elhelyezkedésre, telephelyekre, az egyes besorolásokra, és egyéb szempontokat figyelembe véve kell kialakítani, megtervezni.

Megállapítottuk eddig, hogy a „megfelelő védelem” kontextusában vizsgálandó a jelszó (azonosítás-hitelesítés) területe. Tökéletes védelem nem létezik, ugyanakkor a kiegészítő további kontrollok kialakítása, azoktól való eltérés mérése is rendkívül fontos. Mindezek összességében befolyásolhatják a védelem erősségét. Minden „megfelelő védelem” csak annyira „jó”, mint amennyire képes a célját ellátni. Vagy amennyire képesek vagyunk „gyorsan” érzékelni az esetleges eltéréseket.

A mérésre alkalmazható lista nincs prioritási sorrendben rendezve, mivel, ahogy már fentebb már utaltam rá, annak súlyozása az adott munkaszervezet feladata. Az alábbiakban közreadott listaelemek kiindulási pontként szolgálhatnak ilyen mérésekhez. Fontos megjegyeznem, hogy a kvantifikálás érdekében az egyes sorokat érdemes még kisebb kérdésegységekre, továbbbontani, súlyozni. Ennek oka, hogy pontosabb mérési eredményeket kaphassunk, valamint, hogy a nem egyértelműen igen-nem válaszokat mégis mérhetővé lehessen tenni (operacionalizálás, kvantifikálás fázisai).

A felmérés során az adott (például) szabályozás megléte 1, míg annak hiánya 0 ponttal jelölhető. Így a végén kiadott szám a kérdések összegzett számához viszonyítva százalékos eredményt ad.

Az egyes kérdéseknél jelen cikkben nem került sor példa bemutatására, és a jelszóval, jelszóhasználattal, jelszó elleni tipizált támadási formákkal való összefüggés sem kapott indoklást. Azonban szinte minden esetben megadható lenne ilyen illusztráció, például a véletlen (random) függvény alkalmazásánál is. Amennyiben a megírt kód, az alkalmazott függvény nem került bevizsgálásra, jelentősen lecsökkentheti az adott számteret. Például gondoljunk vissza a három számjegyes számkódos biciklizárra, ahol a lehetséges kombinációk száma legfeljebb 1000 (000-

999). [9] Számos ismertté vált sérülékenység alapja a nem megfelelően inicializált vagy nem bevizsgált random függvény használatára vezethető vissza.

Értékelés alá vont terület	Részterülete	Támpontok a méréshez, kiértékeléshez	Kiértékelés	Súlyozás	Eredmény
A szabályozási környezet	szabályozási környezet megléte	Formális szabályozási környezet, kiadási folyamat, hozzáférhetőség.			Kiértékelés x Súlyozás
	életciklusa	Létrehozás, szakmai köröztetés, felülvizsgálat, érdekelt felek bevonása, dokumentált információ fenntartása, egyéb.			
	részletessége, kezelt területek, beltartalmi vizsgálata	Egységesen minden egyes információs rendszeren és minden munkafolyamatban érvényre juttatható-e; Amennyiben nem, akkor a szabályzat hogyan kezeli a kivételeket, ennek dokumentáltsága.			
	érthetősége, oktatás és vizsgáztatás	A szabályzat elérhetősége. Hogyan történik a kihirdetése, oktatása. Dokumentált információk fenntartása. A felmerült kérdésekkel kihez fordulhatnak a munkavállalók. Vizsgáztatás, eredmények visszacsatolása.			
	életciklusa, felülvizsgálata	A szabályzat életciklus-kezelése. Érdemi felülvizsgálat, köröztetés megtörténte.			

3. táblázat: A szabályozási környezet lehetséges operacionalizálása és kvantifikálásra, forrás: saját szerkesztés

A szabályozási környezet operacionalizálására és kvantifikálásra alkalmas táblázat egy részét, amely a szabályozási környezetre vonatkozik, a 4. számú táblázat mutatja be.

Tisztában kell lenni azzal, hogy a közigazgatásban vagy a 2013. évi L. törvény által érintett munkaszervezetek között természetesen vannak különbségek. Ezek közül több egyértelműen megállapítható, például geolokációs (fővárosi-vidéki), a munkaszervezet nagysága, a munkavállalók eloszlására, kapcsolatba kerülnek-e alkalmazottak direkt módon „ügyfelekkel", biztonsági besorolás stb. Ezért a jelen kiindulási mérési támpont nem tekinthető véglegesnek. Egyrészt az érintett munkaszervezetek között lehetnek olyan különbségek, mely miatt egyes kérdések súlyozottabban, magasabb pontszámmal javasolt, hogy számításba kerüljenek.

[9] https://www.owasp.org/index.php/Insecure_Randomness

Annak érdekében, hogy a magyar közigazgatásban absztrakciós szinten létrejöhessen az információbiztonsági szint mérése, fejlesztése, minden bizonnyal a megfelelő szervezeti, szervezési (jogszabályi) háttér megteremtése javasolt. Kiemelt jelentőségűnek ítélem az információbiztonság területén nemzeti kiberbiztonsági szempontból, hogy központi szinten megvalósuljon a mérés. Hiszen a mérés nélkül nem vehetőek észre a változások, a fejlesztendő területek nem azonosíthatóak.

A szabályozott környezet, annak dokumentált elfogadottsága és ennek megfelelően mély és elvárható rendszerességgel történő oktatása, számonkérése nélkül talán el se várható, hogy az adott munkavállaló tisztában legyen a munkájához tartozó, azzal összefüggő információbiztonsági felelősségével.

Miért tekinthető jó indikátornak a jelszóhasználattal összefüggő (kérdőív, interjús) vizsgálat, felmérés? Jól látható, hogy széles spektrumot lefed a napi munkafolyamatok és alkalmazott IT rendszerek tekintetében is. Valamint az információbiztonságot jelentősen befolyásoló tényezőkre, a felhasználói attitűdre is hatással van.

A useable security megközelítés roppant fontos: tegyünk szívünk kezünket, ki örül „Az Ön jelszava lejárt, kérem változtassa meg!" felugró ablaknak? Ennek érdekében az azonosított folyamatokat és rendszereket feltérképezve és megértve (kockázatokat azonosítva) kell kialakítani a határvédelmet. Biztonsági szempontból alapvetően az a jó kiindulási megfontolás, hogy minden program sérülékeny, a kérdés csupán az, hogy mikor és ki találja meg ennek a sérülékenységnek a kihasználási lehetőségét.[10] A biztonságtudatos magatartásnak így mindenre hatása van, hiszen a főbb életcikluselemekről (egyelőre) emberek döntenek.

A szabályzatok meglétén és minőségén kívül számos terület mérhetővé tehető. A gyakorlatban, a hétköznapok során a szabályzat és a gyakorlat összhangja vizsgálandó, amire példát ad az alábbi táblázat.

Értékelés alá vont terület	Részterülete	Támpontok a méréshez, kiértékeléshez	Kiértékelés	Súlyozás	Eredmény
A jelszóhasználat hétköznapi gyakorlata egyes élethelyzetekben, az X. folyamat támogatása.	Az AA folyamat támogatottsága.	Szoftveres, hardveres vagy automatizált támogatottság van-e?			
	A jelszótárolás támogatottsága.	A folyamat támogatása. Szervezési intézkedések. A folyamat oktatása.			

[10] Sérülékeny véletlenszám generátor, amely titkosítási megoldásokra is hatással volt. http://tech.cert-hungary.hu/vulnerabilities/CH-1222

	Kiemelt jogosultságokra alkalmazott elvárások.	Kiemelt jogosultságokra külön definiáltak-e elvárások? Beszállítói elvárások.			
	Rendszerek átvétele, beüzemelése.	Alapértelmezett hozzáférések kezelése. Hozzáférési szintek és hozzáférések kialakítása, birtokba adása. Biztonsági kialakítás.			
	A perimétéren megjelenő információk figyelése, elemzése.	A szervezetet érintő információk figyelése, elemzése, threat hunting.			
	Jelszóéletciklus.	Kiadása, felügyelete, változtatási kérelmek, életciklus-kezelés.			
	Kezelés, kivételek, élethelyzetek kezelése.	Előfordul-e, hogy a munkavállalók megosztják a jelszavakat?			
		Előfordul-e, hogy adott munkaszervezeti vezető leíratja, kiadatja a munkavállaló jelszavát?			
		Egyéb olyan tényező ismert-e, amikor más jelszava ismertté válhat (pl.: jelszókiadás, jelszóváltoztatás stb. munkafolyamatokban)? Helyettesítés, nyaralás, egyéb élethelyzetek kezelése.			
		Kiadást követő felügyelet.			

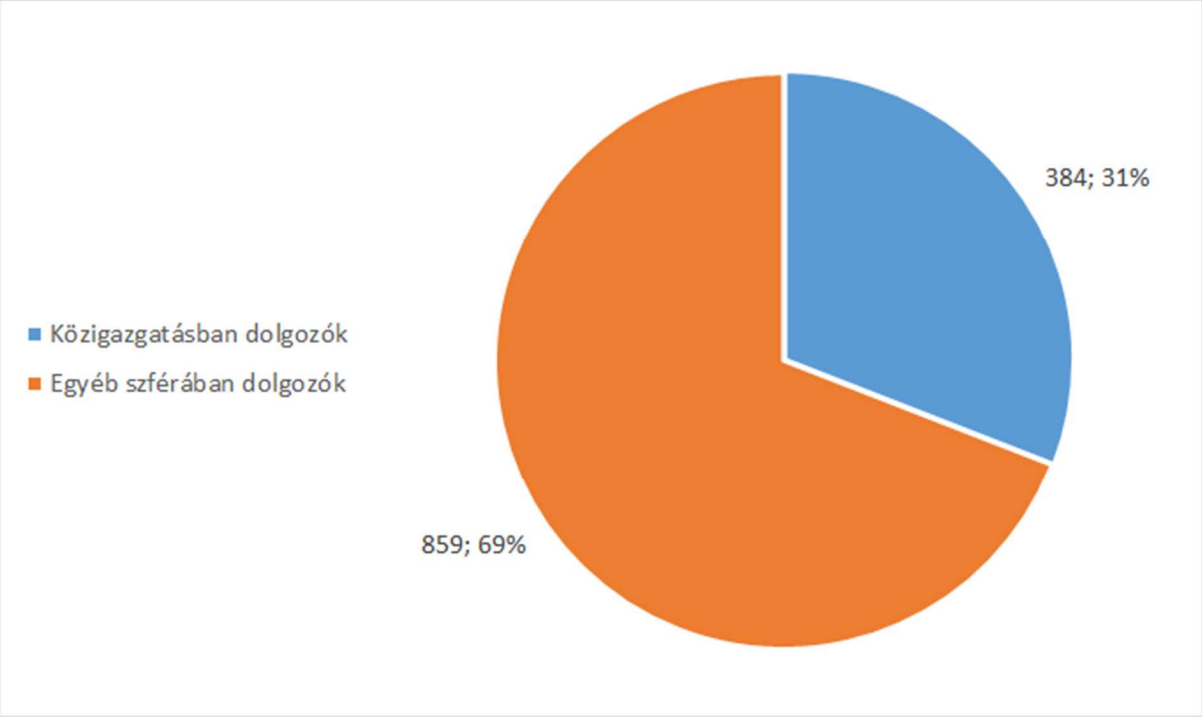
4. táblázat: A jelszóindikátor kiértékelése, forrás: saját szerkesztés

Megfigyeléseim szerint tehát jelenleg nincs a 2013. évi L. törvény hatálya alá tartozó szervezetek mindegyikében egységes mérési módszertan kidolgozva, alkalmazva az információbiztonsági szint mérésére. Erre vonatkozó ajánlás csak a régebbi ajánlásokban szerepelt. Az egyes elszigetelt mérések nem összevethetőek. Ahol készülnek is mérések, ott sem garantált, hogy minden évben megtörténik a mérés megismétlése. Mindezek miatt az érintett (közigazgatási) szervezetek információbiztonsági szintjéről, valamint annak változásáról nincs jelenleg egzakt, számszerűsíthető adat. Ebből következik, hogy jelenleg annak fejlesztésére sincs egységes, bizonyítottan működő módszertan alkalmazva. Illetve az egyes helyeken működő, esetlegesen egyes területeken bevált gyakorlatok továbbra is szigetszerűek maradnak. Megfigyeléseim szerint a 41/2015. BM rendelet által előírt oktatások nem valósulnak meg elvárható gondossággal a szervezetek jelentős részében. A háromféle (új belépőknek szánt, szerepkör alapú és incidenskezelési) előírt oktatás eltérő mértékben valósul meg az egyes munkaszervezetekben.

Ennek érettségi szintje tapasztalataim szerint az általános információbiztonsági szinten erős lenyomatot képezhet.
Szükséges és égető kérdés lehet egy nemzeti információbiztonsági koncepció mentén a méréshez szükséges feltételrendszer megteremtése, a mérés (operacionalizálás, kvantifikálás), kiértékelés egységesítése, központi megvalósítása és a források megteremtése.

4.1.1. ONLINE KÉRDŐÍV ELEMZÉSE

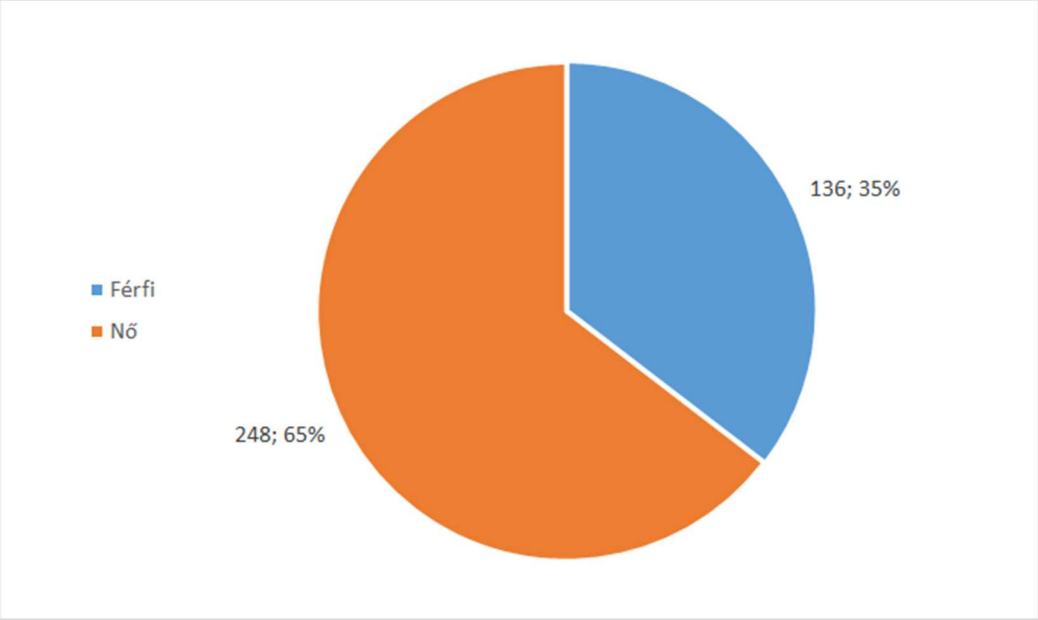
A kutatásom kérdőívének kitöltésére 2014. decembertől 2015 júliusáig volt lehetőség az egyedi linkeken keresztül. Így ezek után azt vizsgáltam meg, hogy az általam online megkérdezettek milyen szférában dolgoznak, mennyi adatot tudok a közigazgatásban végzett szegmens értékeléséhez felhasználni. Ezt az eloszlást mutatom be a 16. számú ábrán.



16. ábra: Az online kérdőívkitöltők szféra szerinti eloszlása, forrás: saját szerkesztés

A fenti ábráról leolvasható, hogy az 1243 válaszadó közül 384 fő közszférából érkező válaszadó, valamint 358 fő az üzleti szférát jelölte meg – az így adott válaszokat, így szolgáltatott szakmai adatokat vizsgálom kutatásomban.

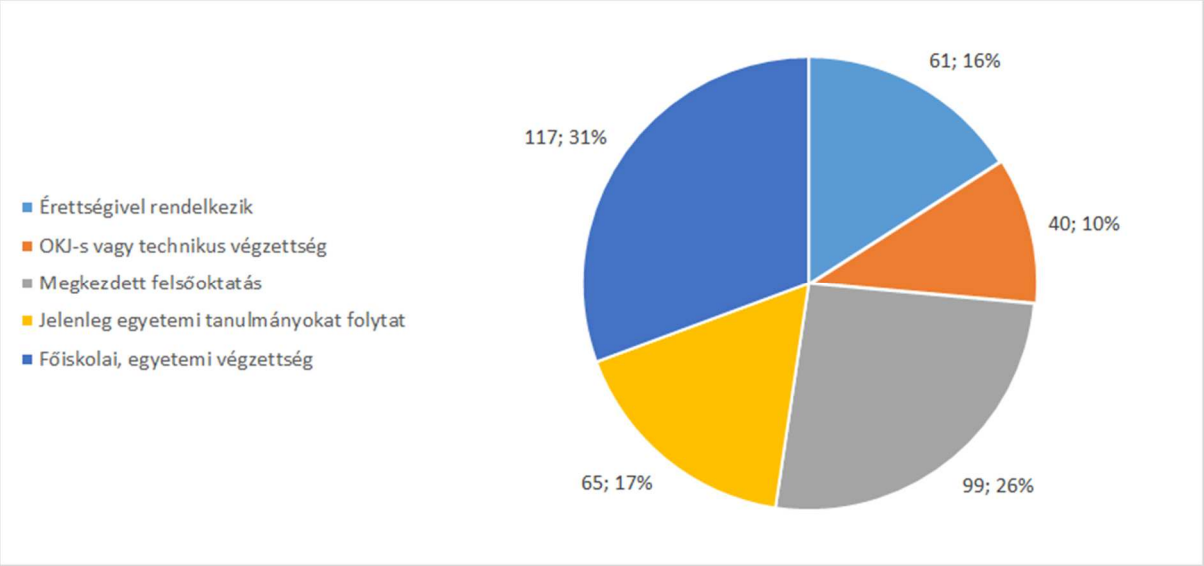
A kérdőívben rendelkezésre álló demográfiai adatokat is elemeztem, ezeket mutatom be a következőkben.



17. ábra: Az online kérdőívkitöltők nem szerinti eloszlása közigazgatáson belül, forrás: saját szerkesztés

A 17. számú ábrán az látható, hogy a közigazgatásban dolgozó kitöltők mintegy 35%-a férfi, 65%-a pedig nő volt.

A demográfiai adatokat az egyes szférákon belül, így az üzleti szférán belül külön vizsgáltam. Az üzleti szférában dolgozó kitöltők mintegy 16%-a nő, 84%-a pedig férfi volt, 299 férfi és 59 női kitöltő volt.
Vizsgáltam az iskolai végzettséget a közigazgatási szférán belül. Ezt mutatom be a következőkben.

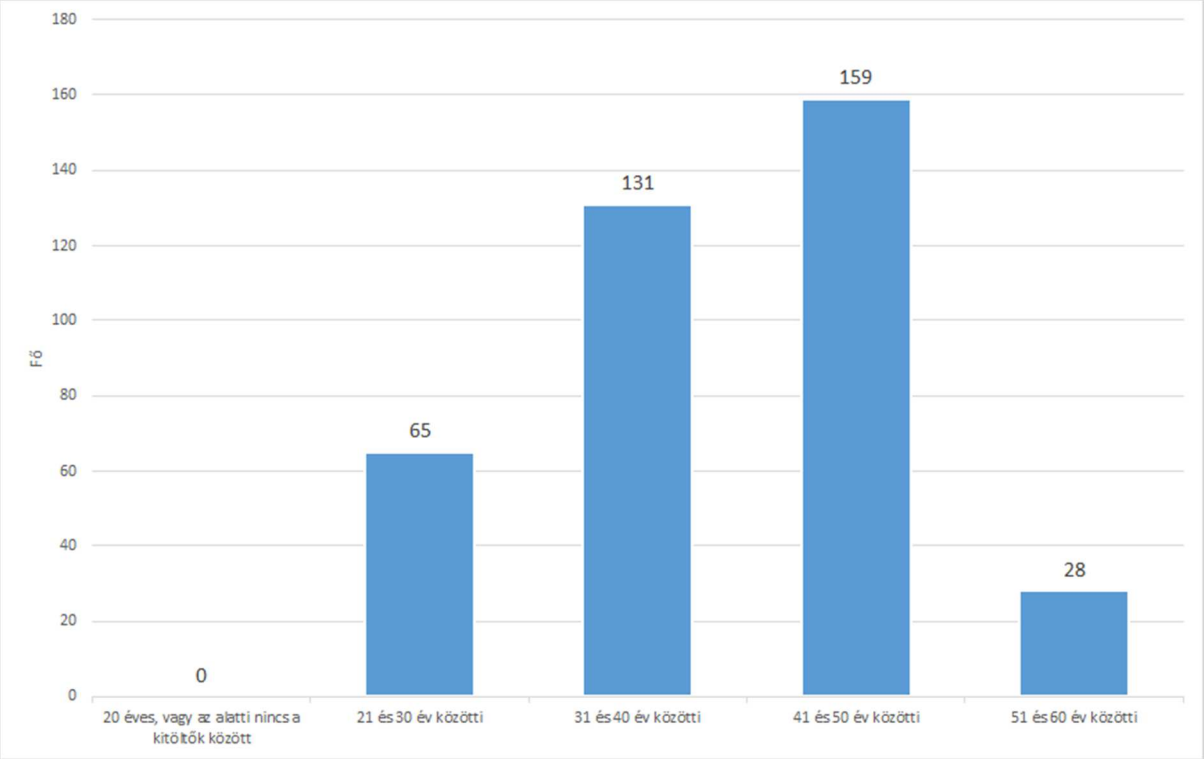


18. ábra: Az online kérdőívkitöltők végzettség szerinti eloszlása közigazgatáson belül, forrás: saját szerkesztés

A 18. számú ábrán látható a közigazgatásban dolgozó válaszadók végzettség szerinti eloszlása, ahol feltüntettem a darabszámokat és a százalékos arányokat.

Érettségivel rendelkezik	61 fő
OKJ-s vagy technikus végzettség	40 fő
Megkezdett felsőoktatás	99 fő
Jelenleg egyetemi tanulmányokat folytat	65 fő
Főiskolai, egyetemi végzettség	117 fő

A kérdőív demográfiai blokkjában, annak 1.2 alpontjában bekértem a születés évét, majd ebből került meghatározásra az életkor. Életkor szerint vizsgálva a közigazgatásban dolgozó kitöltők eloszlását 23 és 68 éves kor között helyezkednek el. Az így kapott adatokból készítettem diagramot.



19. ábra: Az online kérdőívkitöltők életkor szerinti eloszlása, blokkosítva, forrás: saját szerkesztés

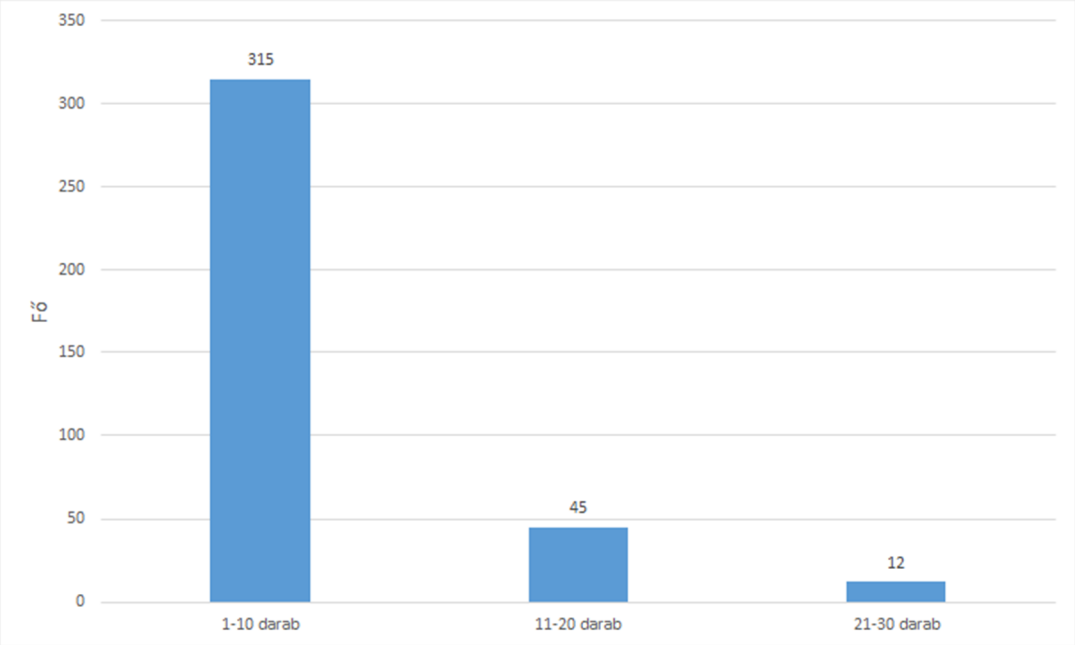
A 20. számú ábrán a közigazgatási szférán belül vizsgáltam az életkor szerinti eloszlást, blokkosítva leolvasható, hogy 20 éves vagy az alatti nincs a kitöltők között:
21 és 30 év közötti: 65 fő,
31 és 40 év közötti: 131 fő,
41 és 50 év közötti: 159 fő,
51 és 60 év közötti: 28 fő volt a válaszadók között.

A kérdőív demográfiai adatait követően a 2-es blokkban a jelszóhasználattal mint az információbiztonság lehetséges indikátorával kapcsolatos kérdések következtek. Disszertációmban ahogy arra utaltam már, természetesen más indikátorok és mérőszámok is lehetnek, amelyek az egyén vagy a munkaszervezet információbiztonsági szintjéről, lehetséges kockázatokról tudnak számszerűsíthető értéket szolgáltatni. Ebből az egyik a kutatásaim során vizsgált jelszókezelés, amellyel kapcsolatos szokások olyan jelentős kockázatokat hordozhatnak, hogy alkalmas indikátorként az információbiztonsági szint számszerű jellemzésére.

A közigazgatásban dolgozók mintáján vizsgálom az alábbi kérdéseket, összehasonlítva az üzleti szférát megjelölt kitöltők által megadott adatokkal.

A 2.1-es “Hozzávetőlegesen hány darab különböző jelszót használsz?” kérdést vizsgálom a következőkben. Mivel az jelszóhasználati szokások jó indikátornak tekinthetőek, így annak darabszámára vonatkozó kvantitatív információ jó kiindulási pont lehet.

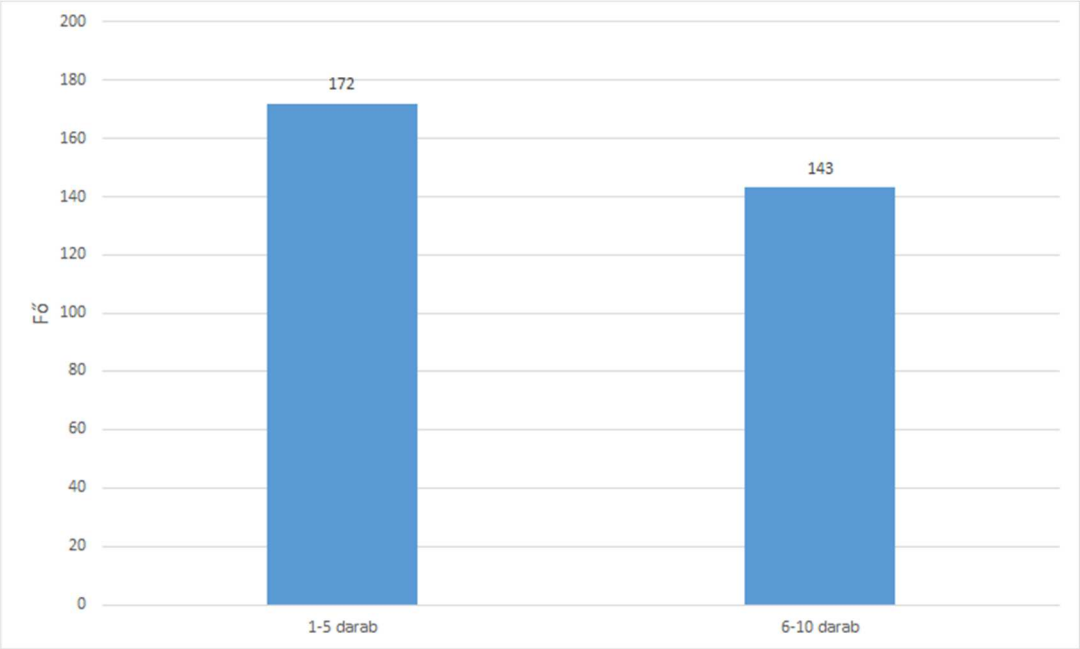
2.1 Hozzávetőlegesen hány darab különböző jelszót használsz?



20. ábra: A közigazgatáson belüli jelszódarabszám-eloszlás, forrás: saját szerkesztés

A 20. számú ábrán blokkosítva ábrázolom, a jelszódarabszám eloszlását. Leolvasható, hogy
315 fő használ 1-10 darab közötti jelszót,
45 fő használ 11-20 darab közötti jelszót,
12 fő használ 21-30 darab közötti jelszót.

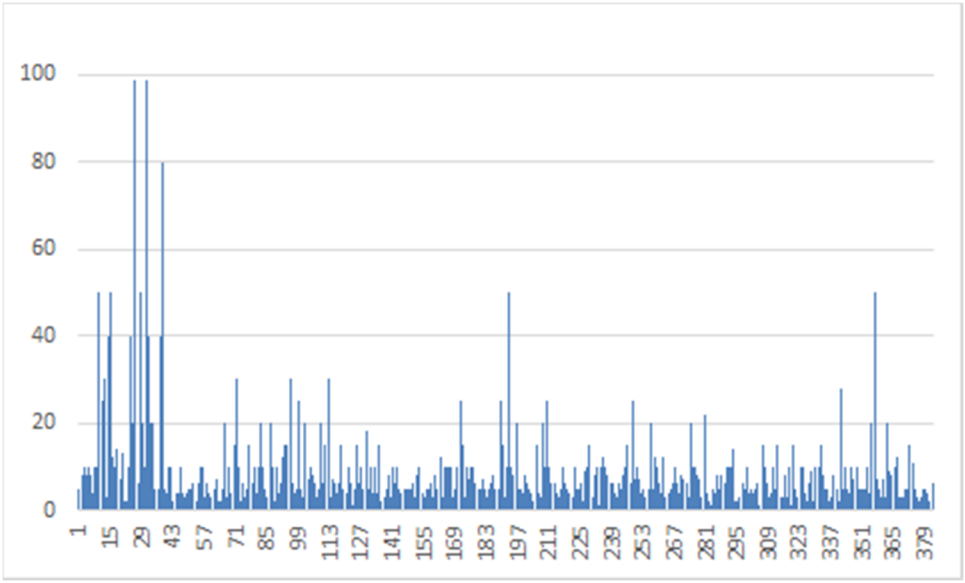
Mivel az első 10-es blokkban nagyon magas volt a válaszadók száma, így azt alaposabban, kisebb intervallumokra bontva is megvizsgáltam.



21. ábra: A közigazgatáson belüli jelszódarabszám-eloszlás más blokkméretben, forrás: saját szerkesztés

A 21. számú ábrán látható, hogy az 1-10 darab jelszót használók körében többségben vannak, akik az intervallum bal oldalához közelítenek, azaz 1-5 darab jelszót használnak. Leolvasható, hogy 172 fő használ 1-5 darab közötti jelszót, 143 fő használ 6-10 darab közötti jelszót.
Az állapítható meg, hogy kevés, kis számú különböző jelszót használnak, és annak is a legnagyobb sűrűsödése az intervallum elején, az 1-5 csoportban mérhető. A hétköznapi élet során jellemzően 5-nél több különböző információs rendszert használunk, így mindenképpen kevésnek tűnik, ha ezen rendszerekhez 5 darab vagy annál kevesebb egyedi jelszó kerül alkalmazásra, illetve az is következhet, hogy egy vagy több információs rendszerhez ugyanaz a jelszó kerül újrafelhasználásra, ami komoly biztonsági kockázatot jelenthet.

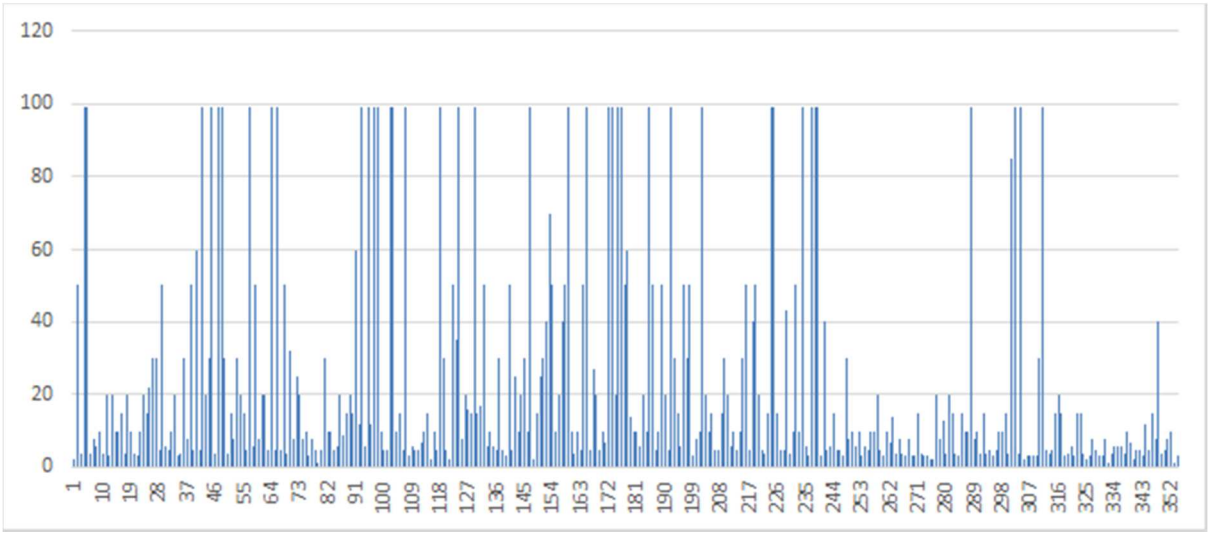
Ezek után a jelszóhosszúság megoszlását is vizsgáltam a közigazgatási mintában.



22. ábra: Jelszóhosszúság-eloszlás a mintában (közig.), forrás: saját szerkesztés

A 22. számú ábrán a függőleges tengelyen a jelszóhosszúság van ábrázolva, a vízszintes tengelyen az egyes válaszadók által megadott értékek és az látható, hogy a közigazgatásban dolgozó válaszadók többségének, ránézésre és egy-egy kiugró értéktől eltekintve 20 alatti. Egészen pontosan a közigazgatási mintán vizsgálva az átlagos jelszódarabszám 9,34 darab.

Az üzleti szférában, azon a mintán vizsgálva az átlagos jelszódarabszám 23,42 darab. Ennek eloszlását mutatja az alábbi ábra.



23. ábra: A jelszóhosszúság eloszlása a mintában (közig.), forrás: saját szerkesztés

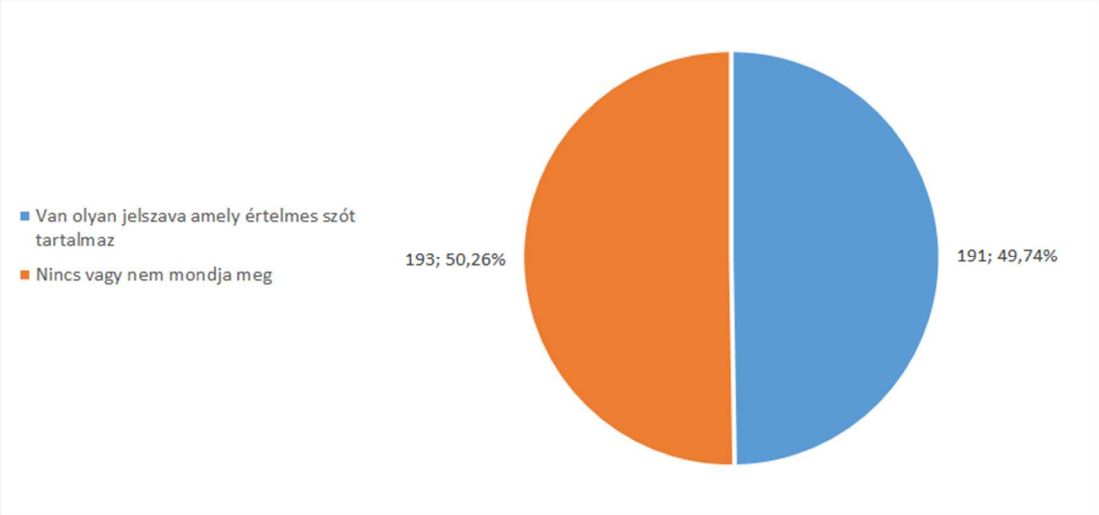
Az 23. számú ábrán az látható, hogy míg a közigazgatási mintában kevesebb kiugró érték volt, az üzleti szférában számos (jelentősen hosszabb jelszó) kiugró érték található.

A függőleges tengelyen a jelszóhosszúság van ábrázolva, a vízszintes tengelyen az egyes válaszadók által megadott értékek. Arra is lehet következtetni, hogy mivel minden bizonnyal nem

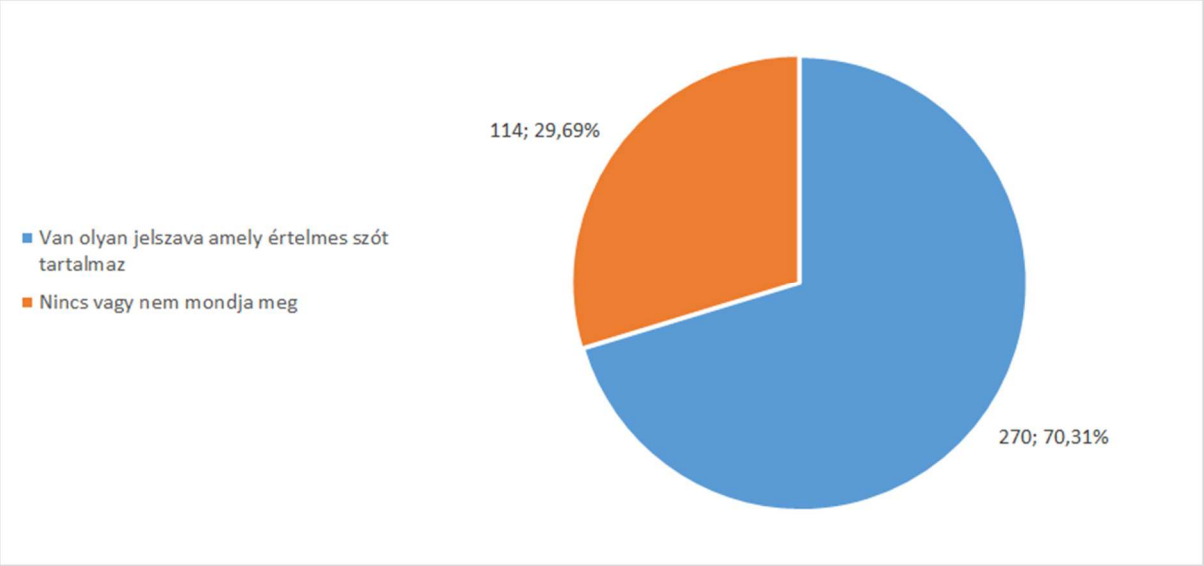
lehetséges fejben tartani több tucat vagy 100 darab különböző jelszót, így ezen válaszadók feltételezhetően jelszószéfet vagy valamilyen más megoldást alkalmazhatnak a jelszavak kezelésre. Ez egy egészen más tudatossági és/vagy technikai tudást feltételez.

A 2.1-es "Hozzávetőlegesen hány darab különböző jelszót használsz?" kérdésnél tehát különbség mutatkozik a közigazgatás és az üzleti szféra között. Továbbá a közigazgatási mintában a legrövidebb, az 1-5 darab különböző jelszó blokkban található a legnagyobb sűrűsödés. Az üzleti szférában dolgozók körében több mint kétszer olyan nagy nagyságrendben használnak különböző jelszavakat.

Ezt követően a kérdőív 2.2-es "Van-e olyan jelszavad, ami tartalmaz személynevet?" és a 2.3-as "Van-e olyan jelszavad, ami tartalmaz értelmes szót akár magyarul vagy bármely más nyelven?" kérdésnek kiértékelését összevontam, és elemeztem a közigazgatásban dolgozók válaszait.



24. ábra: Személynevet vagy értelmes szót tartalmazó jelszavak aránya az üzleti szférában. forrás: saját szerkesztés



25. ábra: Személynevet vagy értelmes szót tartalmazó jelszavak aránya a közigazgatási mintában, forrás: saját szerkesztés

A 24. számú és 25. számú ábrákon az látható, hogy jelentősebb mértékben válaszolták azt a közigazgatásban dolgozó válaszadók, hogy a jelszavuk tartalmaz valamilyen értelmes szót. Az értelmes szót tartalmazó jelszavak használata azt a kockázatot rejti magában, hogy akár hashből visszafejtés, akár más kompromittálódási kockázatnak való kitettsége jelentősen magasabb, mint a mind a 4 szekvenciát tartalmazó random, de legalábbis értelmes szót nem tartalmazó jelszavaké. A 384 közigazgatásban dolgozó kitöltő közül magas arányban, 191 kitöltő mondta, hogy van olyan jelszava, amely tartalmaz személynevet, és 18 fő választotta a "nem mondom meg" lehetőséget. Azaz a felhasználók 49,73%-a személyneveket tartalmazó jelszót vagy jelszavakat használ. Ez egyébként egybevág (Som-Papp, 2015, Hungarian trends of password usage) és Tihanyi (2013) kutatásaival. Ez a gyakorlat azért számít rendkívül rossznak, magas kockázatot rejtő gyakorlatnak, mivel az értelmes szótári szavakat, így például a tipizálható magyar (anyakönyvezhető) személyneveket vagy akár a rövidebb jelszavakat, nem minden lehetséges szekvenciát tartalmazókat könnyebben lehet visszafejteni, kompromittálni. Az értelmes szót tartalmazó jelszavak esetében az ilyen válaszok aránya még ennél is magasabb, 70,31% volt.

A 2.4 - 2.7 kérdésekkel "A jelszavamtól elvárom, hogy ...legyen biztonságos. ...legyen megjegyezhető. ...feleljen meg a jó jelszó elvárásainak. ...meg tudjam védeni az adataimat"; annak feltárása volt a cél, hogy hogy milyen preferenciákat részesítenek előnyben a válaszadók.
A közigazgatás és az üzleti szféra válaszait összehasonlítva látható, hogy eltérő súlyozással válaszoltak, eltérő súllyal veszik figyelembe az egyes jelszóminőségi, információbiztonsági

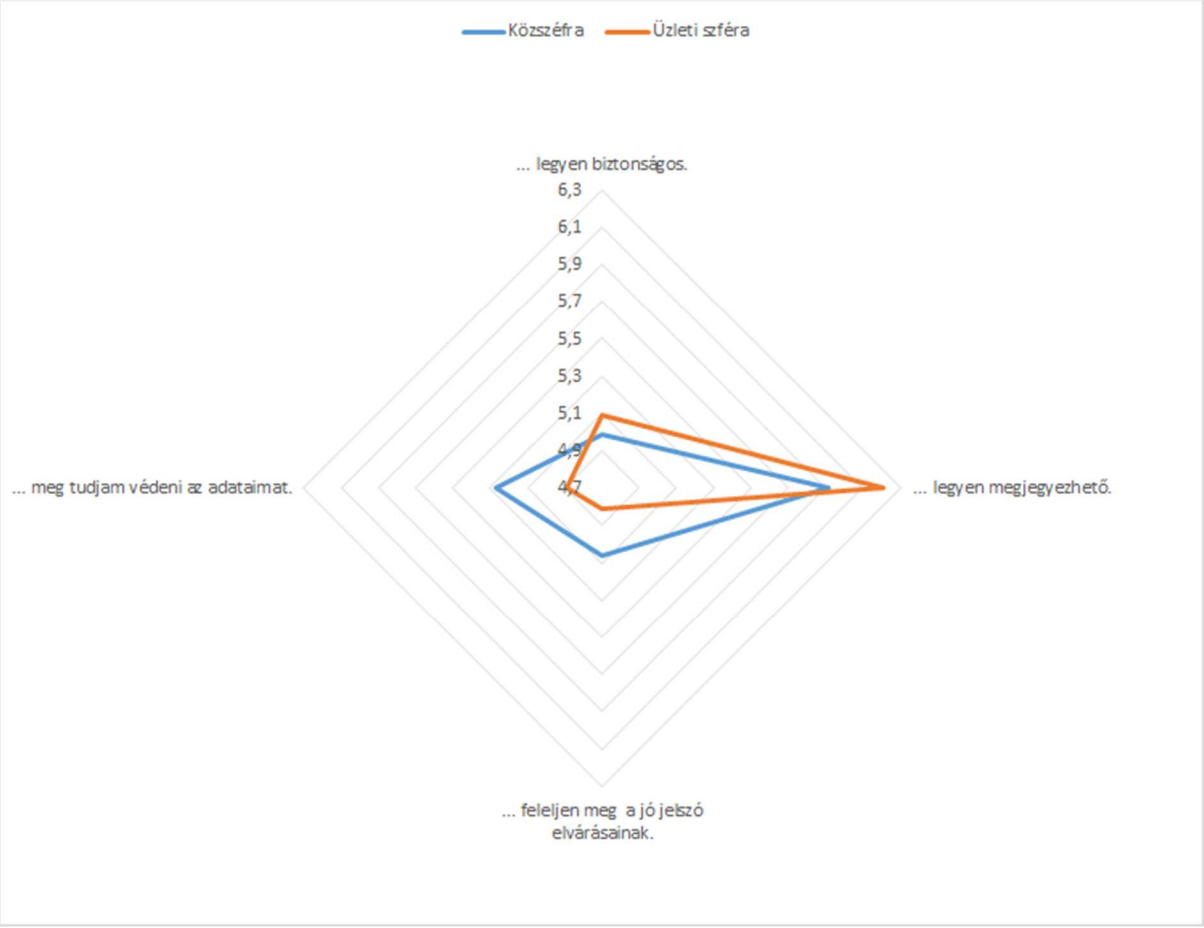
kritériumokat. Egy 0-6 fokozatú skálán az alábbi értékek születtek átlagosan a közigazgatás és üzleti szféra viszonylatában.

Átlagos értékek, adott szféra vonatkozásában	... legyen biztonságos.	... legyen megjegyezhető.	... feleljen meg a jó jelszó elvárásainak.	... meg tudjam védeni az adataimat.
Közszéfra	4,99	5,92	5,06	5,27
Üzleti szféra	5,09	6,21	4,81	4,89

5. táblázat: "Mit várok el a jelszavamtól?" kérdésre adott válaszok szféránként, forrás: saját szerkesztés

A 5. számú táblázatban összehasonlítom a közigazgatási és üzleti szférában dolgozók által kapott válaszokat.

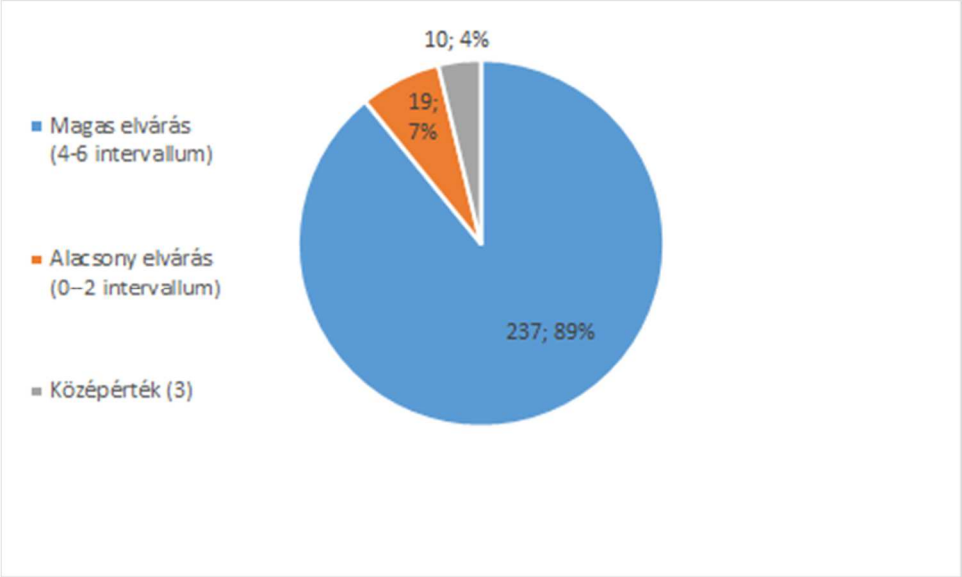
Az így kapott értékeket vizuálisan, sugár diagram segítségével mutatom be.



26. ábra: "Mit várok el a jelszavamtól?" kérdésre adott válaszok nagyságrendje, forrás: saját szerkesztés

A 26. számú ábráról leolvasható, hogy a megjegyezhetőség és biztonság irányába tolódik el a narancs színű alakzat, míg egy idealizált holisztikus megközelítés felé a képen a kék alakzat.

Megfigyelhető, hogy a válaszadók többségének alapvetően magas az elvárása, az intervallum jobb oldalára tolódik, ezt szemléltetem vizuálisan is.



27. ábra: Válaszadók elvárásai a jelszavukkal kapcsolatban, forrás: saját szerkesztés

A 28. számú ábrán az látható, hogy a többségnek, 89%-nak magas elvárásai vannak a jelszavával kapcsolatosan. Azonban rendkívül szembetűnő, hogy annak ellenére, hogy 89% azt vallja, hogy 2.4 "A jelszavamtól elvárom, ... hogy legyen biztonságos.", ugyanakkor a már eddigiekben kielemzett kérdésekben, a jelszót mint indikátort kezelve látható, hogy a jelszóval kapcsolatos minőségi elvárások nem teljesülnek, annak hossza, bonyolultsága, egyedisége, valamint darabszáma nem megfelelő. Ezek mindegyike külön-külön is jelentős kockázatot jelent. Összességében pedig a szabály vagy szabályozás ismeretének hiányát vagy annak meg nem értését, el nem fogadását jelentheti.

Ebből ismét arra következtetek, hogy bár fontosnak tartanák a válaszadók a biztonságos jelszavak használatát, akár a szabályzatok ismeretének hiánya, akár az oktatás hiánya vagy a folyamatokban való alkalmazhatóság ismeretének hiánya miatt a magas elvárásoknak való megfelelés módját vagy nem ismerik, vagy belső (tudásbeli) okok miatt nem tudják alkalmazni, vagy az adott folyamataikban nem tudják alkalmazni.
Feltételezhető, hogy így nincs ismeretük a helyes, jó, követendő gyakorlatról, illetve látható, hogy más szférával összevetve komoly eltérés tapasztalható: a közigazgatási értékek elmaradnak a 2.4-es kérdés esetében.

A 2.5 "A jelszavamtól elvárom, hogy ...legyen megjegyezhető." kérdésre az üzleti szférában szintén a fentebb bemutatott magasabb értéket kaptam. Közszféraátlag: 5,92, üzleti szféra: 6,21.

A 2.6 "A jelszavamtól elvárom, hogy ...feleljen meg a jó jelszó elvárásainak." és a 2.7 "A jelszavamtól elvárom, hogy ...meg tudjam védeni az adataimat." kérdésekre a tendencia

megfordul. Ennek okát sokáig kerestem, és a jelszóhossz és a jelszószéf ismeretével találtam összefüggést: azaz ha a jelszóval, annak kezelésével kapcsolatos tudás rendelkezésre áll, például arra vonatkozó tudás, hogyan tudom kezelni, létrehozni. Azaz például saját módszer új jelszó készítésére, vagy a jelszószéf ismerete, vagy az átlagtól jelentősen hosszabb jelszó 15+ karakter, akkor ezek magától értetődőek, hiszen a jelszókezelő rendszer vagy saját algoritmusunk ezeket garantálja. Ezen értékek pedig összevágnak a fentiekkel, hogy az üzleti szférában az átlagos jelszóhossz és jelszó darabszám olyan értékeket mutatott a válaszadók jelentős részén, amely kizárja, hogy ezen jelszavakat fejben, vagy kézzel kezeli. Azaz a bár alacsonyabbnak tűnő értékeket adtak az üzleti szféra válaszadói, de ilyen összefüggésben vizsgálva az következik, hogy kontextusában vizsgálva összességében mégis az üzleti szférában alkalmaznak jobb gyakorlatot a válaszadók.

Ezt a későbbiekben külön kérdéssel való összefüggésben is, saját tapasztalatommal és a nemzetközi eredményekkel való összefüggése is kimutatható, hogy a IKT-képességek, a informatikai rendszerek elfogadottsága (TAM) is hatással van a tudatosságra, szabálykövetésre. Valamint az adott eszközhasználat képessége is külön tényezőként vizsgálandó, releváns tényező. (Bujdosó, 2015) Ebben a konkrét esetben egyértelműen tetten érhető az összefüggés, a 7 fokozatú skálán az egyes kérdésekre adott válaszok átlaga 6,06 és 6,53 között mozog, az összesített pedig 6,27, rendkívül magas. Százalékosan ez 86 és 93 százalék közötti elköteleződést jelent. Ennek jelentése révén kimutatható, hogy nagyon magasra priorizálják a biztonságot, és ezt kivetítik a jelszóhasználati szokásokra, a jelszóval kapcsolatos elvárásukra is. Azonban az előbbiekben már bemutatott 2.1-2.2-2.3 kérdésekre adott válaszok látszólag ellentmondanak ennek a magas elvárásnak. Ennek okai részben a 2.32 és 2.33 és a 2.35-ös kérdésekre

2.33 “Honnan származnak a jelszóval kapcsolatos ismereteid?” és

2.35 “Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?” kérdésekre adott válaszokban találhatók. Mégpedig, hogy jelszóval kapcsolatos ismeretek, mégha kaptak is oktatást akkor is másodlagos forrása az ismerősök és egyéb információforrások rendkívül magas arányban. Illetve a viszonylag alacsony átképzettéssgel magyarázható.

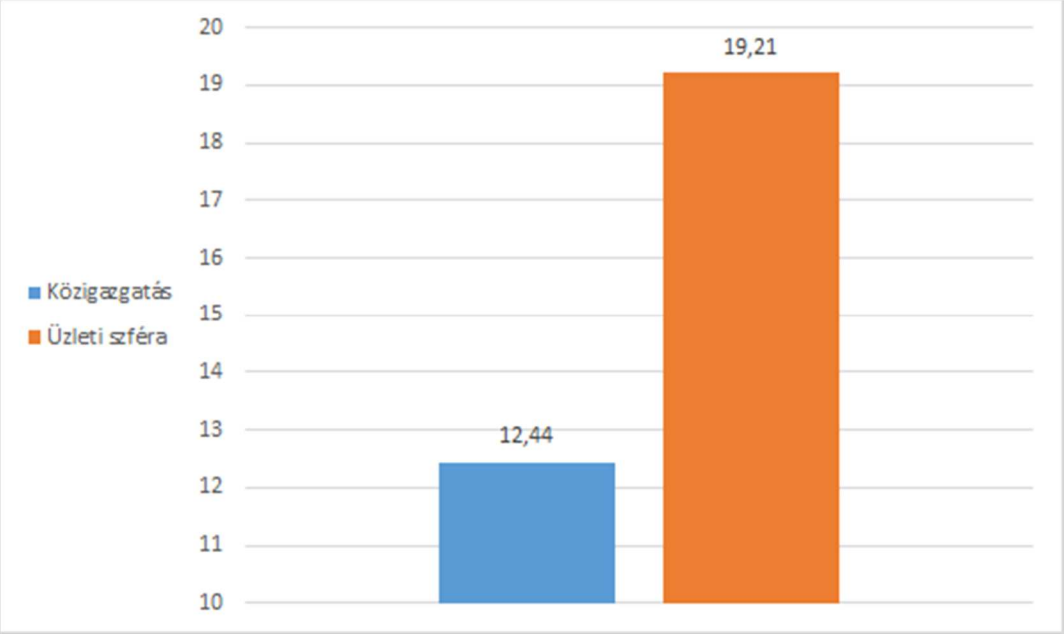
A 2.8 “Hány karakter a legrövidebb jelszavad?” kérdésre a közigazgatásban az átlagos érték: 7,25 az üzleti szférában ez az érték 8,23. Azaz a közigazgatásban átlagosan rövidebb jelszavakat használnak a válaszadók.

A 2.20 “Hány karakter a leghosszabb jelszavad?” kérdésre kapott számszerű válaszoknak az átlagát számítottam a közigazgatási és az üzleti szférán belül, aminek eredményét táblázatban foglaltam össze.

	Hány karakter a leghosszabb jelszavad?
Közigazgatás	12,44
Üzleti szféra	19,21

6. táblázat: Leghosszabb jelszó összehasonlítása szféra szerint, forrás: saját szerkesztés

A 6. számú táblázatban látható, hogy az üzleti szférában dolgozó válaszadók leghosszabb jelszavainak átlaga hosszabb, mint a közigazgatásban dolgozó válaszadóké. Mivel a jelszó hosszúság alapvetően bizonyos kockázatokkal kapcsolatos kompenzációt jelent, így akár 1-1 karakterrel hosszabb is jelentős eredmény lehet. Itt azonban 64,75%-os eltérés, növekedés tapasztalható, az átlagos hosszúság 7 karakterrel hosszabb az üzleti szférában, a közigazgatásihoz képest, jobb gyakorlatot feltételez.



28. ábra: Leghosszabb jelszó összehasonlítása szféra szerint, forrás: saját szerkesztés

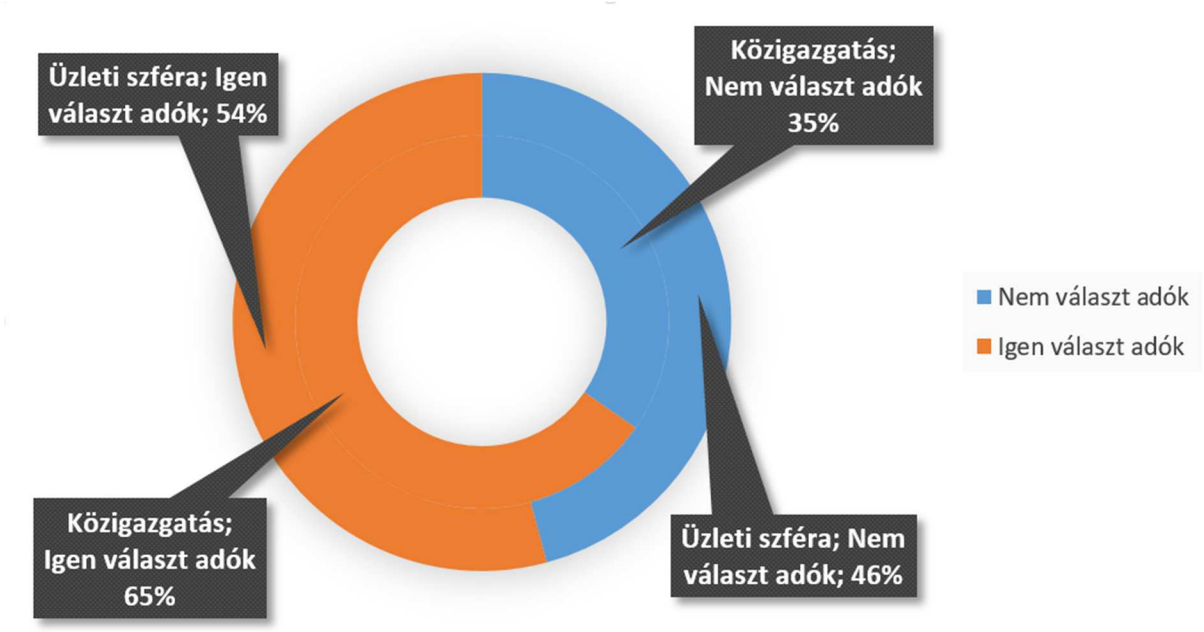
A 28. számú ábrán látható a közigazgatási szférában és az üzleti szférában adott válaszok átlagolása, kiértékelése. Míg a kékkel jelölt közigazgatási szférában a válaszadók átlagos jelszó hossza 12.44 karakter, addig az üzleti szférában ez az érték 19.21 karakter.

A 2.21 “Hány karakter hosszú az, ami nagyon vigyáz az adataidra?” kérdésre a tendencia hasonló:
Közigazgatásban az átlag: 11,31
Üzleti szférában az átlag: 15,81.
Tehát itt is magasabb a karakterszám, a jelszó hosszúság jobb az üzleti szférában dolgozók által alkalmazott gyakorlat.

A trend a 2.22 “Van-e olyan információ, amit fontosabbnak tartasz a többinél, és jobban meg akarod védeni, ebben az esetben hány karaktert használsz?” kérdésben is hasonlóságot mutat.
Közigazgatásban az átlag: 11,06
Üzleti szférában az átlag: 17,18
Tehát a kérdést máshogy, más aspektusból feltéve is az tapasztalható, hogy az üzleti szférában dolgozók hosszabb jelszavakat alkalmaznak általában és egyébként a fontosabb, bizalmasabb adatok, rendszerek védelmében is.

A 2.9 “Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?” kérdésre a közigazgatásban az átlagos érték: 10,14 az üzleti szférában ez az érték 12,99. Azaz a közigazgatásban átlagosan rövidebb a leggyakrabban használt jelszavakat tekintetében is az eredmény. Amennyiben ezt kockázatarányosan közelítjük meg, akkor a közel 3 karakteres különbség igen jelentős, ha annak valamilyen megszerzéséről, vagy visszafejtéséről van szó. Azaz komoly előny, kisebb kockázat, ha hosszabb a jelszó, bár természetesen nem kizárólag a jelszó hosszúsága az egyetlen tényező.

2.10 “Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?” kérdésre az egyes szférákban a válaszadók számának függvényében ábrázoltam, hogy mennyire jellemző, hogy valamilyen értelmes szó, név, kifejezés a jelszó részét képezi.



29. ábra: Jelszavakban előforduló ismétlődő karaktersorozatok vizsgálata szféra szerint, forrás: saját szerkesztés

A 29. számú ábráról leolvasható, hogy 11%-al jobb az üzleti szférában kapott válaszok aránya. Abból kiindulva természetesen, hogy minden rendszerhez egyedi jelszó szükséges, így az a jó, ha adott kifejezés nem ismétlődik a jelszavakban.

Az eredményeket táblázatosan is összefoglaltam.

	Válaszadók összesen	Igen választ adók	Százalék a mintán belül
Közigazgatás	384	251	65,36%
Üzleti szféra	358	194	54,19%

7. táblázat: Ismétlődő karakterek vagy karaktersorozatok, kifejezések előfordulása szféránként (db, %), forrás: saját szerkesztés

Ezt számszerűen a 7. számú táblázatban is összefoglaltam. Egyes szféránként, valamint szférán belül vizsgálva az eltéréseket. Tudvalévő, hogy az ismétlődő karaktersorozatok, az értelmes kifejezések mind ellenjavaltak a jelszóhasználat vonatkozásában. Az látható, hogy az üzleti szférában arányait tekintve is alacsonyabb, azaz a közigazgatásban magasabb, 65%-a a válaszadóknak mondja, hogy van valamilyen értelmes kifejezés a jelszavakban, amely egy káros gyakorlat. Az olvasható le a táblázatból, hogy közigazgatásban ez a kerülendő rossz gyakorlat sokkal magasabb százalékban van jelen.

A 2.14 “Hallottál-e már jelszószéfről (jelszókezelő programokról)?” kérdésre a fentebb már az összefüggések miatt említett kérdésre adott válaszok alapján nagyságrendi különbség van a jelszó kezelés lehetőségeinek ismeretéről, a jelszószéf programok vonatkozásában.

	Válaszadók összesen	Igen válasz, hallott már jelszószéfről	Mintán belüli százalék
Közigazgatás	384	116	30,21%
Üzleti szféra	358	278	77,65%

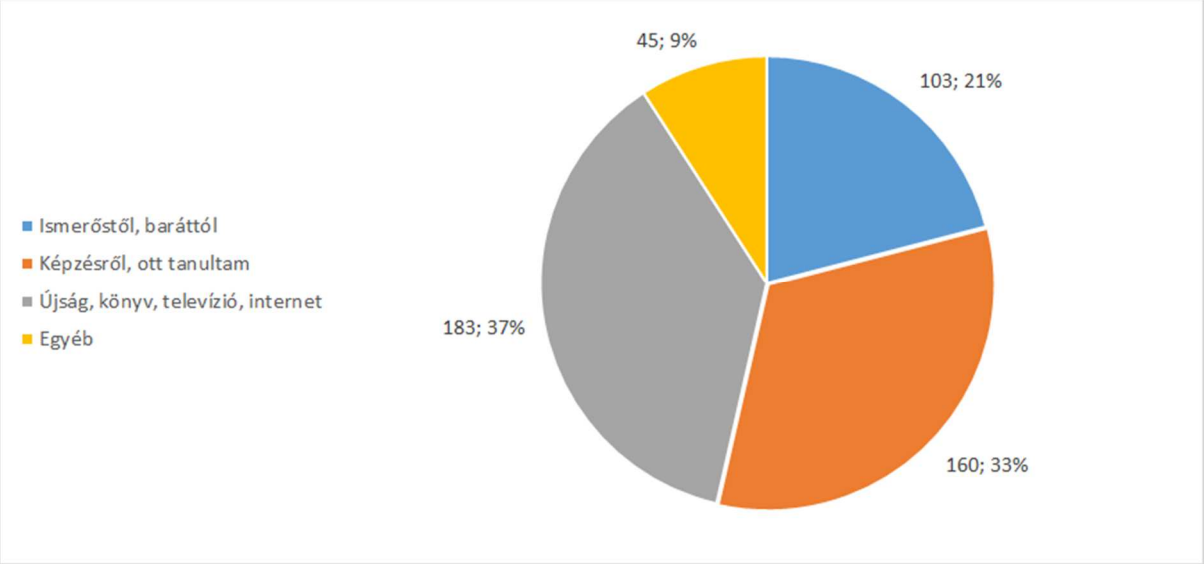
8. táblázat: Jelszószéf-alkalmazás ismerete szféra szerint, forrás: saját szerkesztés

Ez alátámasztja a fentebbi megállapításokat, hogy az eszközök ismerete, növeli a jelszóhasználati szokásokon keresztül az információbiztossági tudatosságot, a szabálykövetést támogatja. Az eddig vizsgált kérdésekhez és eltérésekhez képest is jelentősen nagy a két szféra között az eltérés. Ahogy a 10. számú táblázat mutatja, az üzleti szférában jelentősen többen ismerik a jelszószéf fogalmát, amely nagyobb tudás szintet feltételez.

A 2.32 “Mennyire jellemző, hogy törekszel az erős jelszóra?” kérdésre adott válaszok átlaga 4,92, tehát abszolút a felső harmadba tartozik. A 384 közigazgatási válaszadóból 349 válaszadó jelölt meg az intervallum jobb oldalához tartozó értéket, azaz inkább jellemző, hogy

törekszik az erős jelszóra. Ugyanakkor az üzleti szférában a válaszadók által adott értékek átlaga 5,12, amely magasabb törekvést, elkötelezettséget jelez, mint a közigazgatásban.

2.33 “Honnan származnak a jelszóval kapcsolatos ismereteid? (Több válasz is lehetséges!)” kérdésre adott válaszokat vizualizáltam a közigazgatásban dolgozó válaszadókat dolgozva fel.



30. ábra: Jelszóval kapcsolatos ismeretek forrásainak eloszlása, forrás: saját szerkesztés

A 30. számú ábrán leolvashatóak a válaszadók által arányok is leolvashatóak. Mindenképpen számottevő az oktatás és hírközlési médiumok mellett az ismerőstől, baráttól kapott információk. A kérdésre az alábbi válaszokat kaptam:

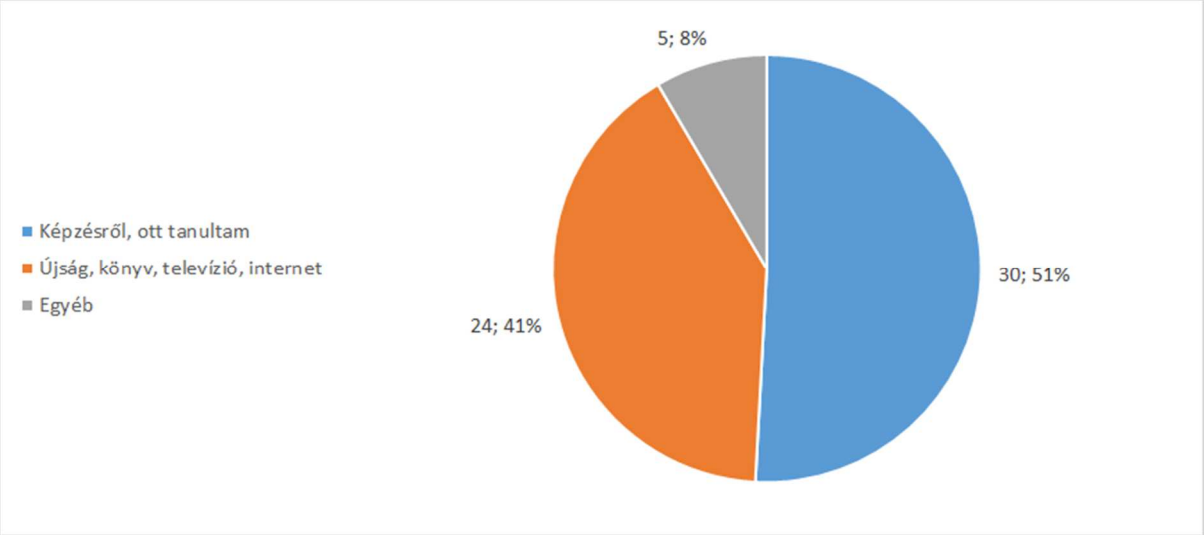
Ismerőstől, baráttól: 103 fő.

Képzésről, ott tanultam: 160 fő.

Újság, könyv, televízió, internet: 183 fő.

Egyéb: 45 fő.

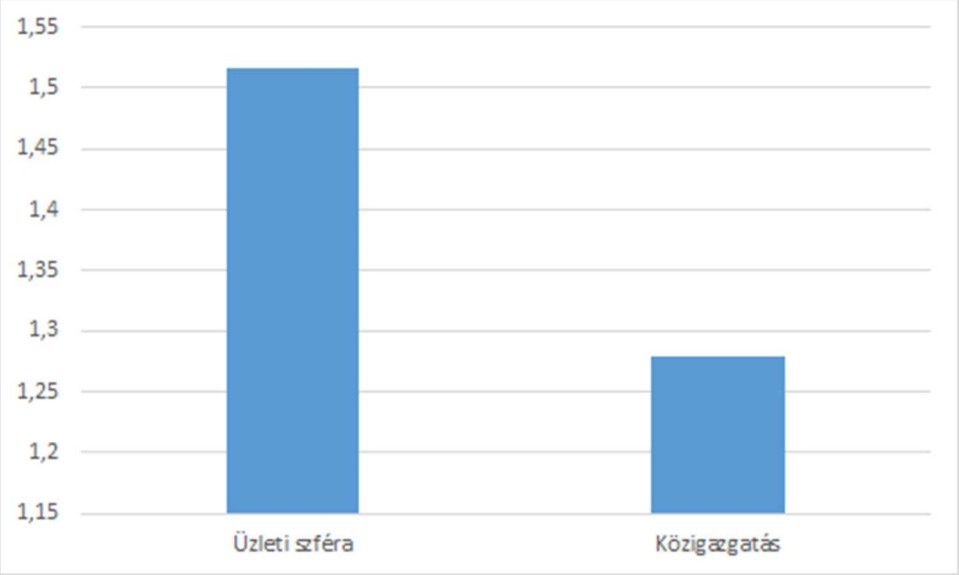
Ha azonban a csoporton belül szűkítést alkalmazok, és azokat vizsgálom, akik ismerőstől, baráttól (is) szereznek jelszóval kapcsolatos ismereteket, akkor az egyébként nem a matematikailag indokolhatónak tűnő közel felezős vagy harmadolós arányszámot kaptam:



31. ábra: Többszörös ismeretforrás mintán belül, forrás: saját szerkesztés

A 31. számú ábrán az látható, hogy akik megjelölték, hogy ismerőstől, baráttól (is) származó információforrásuk, azon válaszadók által még megjelölt további kategóriákat is megjelöltek.

A 2.33-as kérdés alkalmas lehet az értekezésemben már említett csoportnyomás, csoportnorma alátámasztására is. Azaz, minél több helyről szerzi be ismereteit, annál valószínűbb, hogy a kongruens világképbe beleilleszkedik a megfelelő tudatos viselkedés, nem csak robotikus szabálykövetés valósul meg. Így megvizsgáltam, hogy a
közigazgatáson belül 384 fő 491-szer jelölte be, azaz átlagosan 1,27, de egynél több helyről szerzi be ezen ismereteit. Üzleti szférán belül 358 fő 543-szor jelölte be, azaz átlagosan 1,51, de egynél több helyről szerzi be ezen ismereteit.



32. ábra: Többszörös ismeretforrás mintán belül szféránként, forrás: saját szerkesztés

Azaz leolvasható, hogy a minta arányaihoz viszonyítva is 18,62% százalékkal magasabb a nyitottság arra, hogy több helyről szerezze be információbiztonsággal, jelszóval kapcsolatos ismereteit. Ugyanakkor ebből akár az is következhet, hogy könnyebben is osztja meg ilyen jellegű tudását, amely a csoportnorma információbiztonsági növeléséhez, nyíltabb kommunikációhoz és az új belépők információbiztonsági szintjének növeléséhez, szintre hozásához is hozzájárulhat. A közigazgatásban található alacsonyabb számok pedig ennek esetleges hiányáról, vagy alacsonyabb szintjéről árulkodnak.

2.24 "Mennyire értesz egyet a következő állításokkal? Ha megbízható emberekkel használok közös jelszót, az nem jelent biztonsági kockázatot."

Az üzleti szféra válaszadóinak átlaga 2,16, ahol a 0 az "Egyáltalán nem értek egye"t és a 6 "Teljes mértékben egyetértek" lehetőség volt. Tehát inkább a nem értek egyet irányába mozdul, bár így is elég magas. A közigazgatásban ez az érték valamivel magasabb, 2,33 a válaszok átlaga.

A közigazgatásban kapott válaszok alacsonyabb szintet képviselnek információbiztonsági szempontból, mint az üzleti szférában adottak.

2.25 "Mennyire értesz egyet a következő állításokkal? Minden helyre különböző jelszót használok."

Ennél a kérdésnél is a 0 az "Egyáltalán nem értek egyet" és a 6 "Teljes mértékben egyetértek" lehetőség volt.

Az üzleti szféra válaszadóinak átlaga 3,95

A közigazgatásban ez az érték valamivel alacsonyabb 3,59 volt.

Ennél a kérdésnél a magasabb érték tekinthető jobb válasznak információbiztonsági szempontból.

A közigazgatásban kapott válaszok alacsonyabb szintet képviselnek, mint az üzleti szférában adottak.

A fentiekben leírt módon a jelszókezelést az információbiztonsági tudatosság egyik indikátoraként kezeltem. A kiértékelés során indexet készítettem a skálás válaszadási lehetőségek egyik csoportjából. Nyolc változót azonos súllyal szerepeltettem az jelszókezelés-információbiztonsági tudatossági indexben, 1-tól 7-ig skálát alkalmaztam hét esetben, egy esetben pedig transzponáltam a kapott válaszok értékeit, mivel a kérdés (Ritkán változtatok jelszót.) tagadó módban volt feltéve, illetve az egyet nem értés információbiztonsági szempontból az elvárt attitűd.

Az indexkészítéshez felhasznált kérdések az alábbiak voltak:

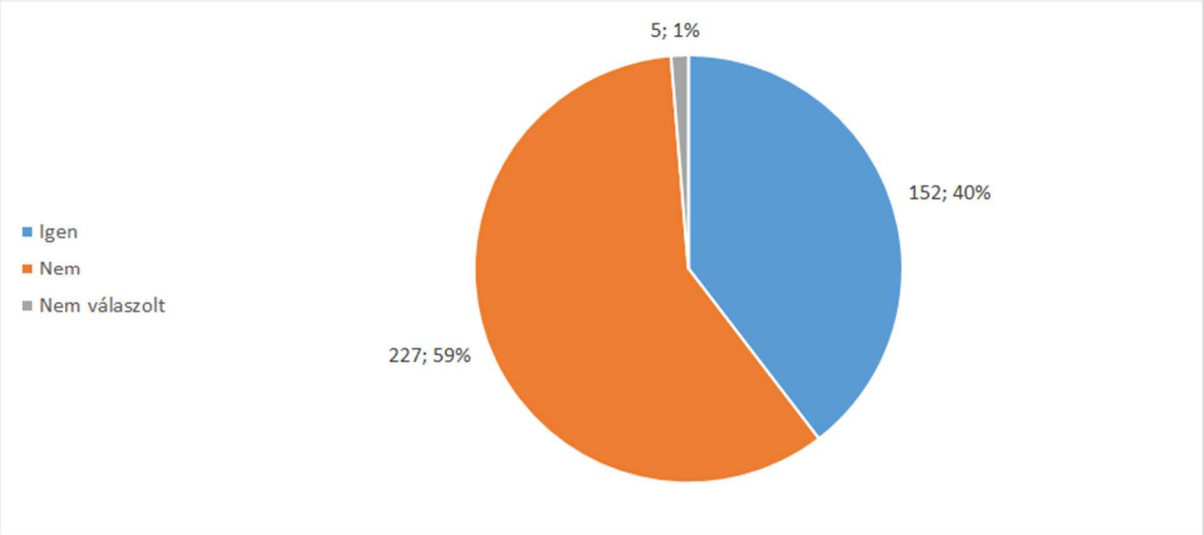
2.25 "Minden helyre különböző jelszót használok."

2.26 "Ritkán változtatok jelszót." (transzponált értékekkel)

2.27 “Jelszavaimban általában mind a 4 karaktertípust (kisbetű(ke)t, nagybetű(ke)t, számo(ka)t és speciális karakter(eke)t) használom.”
2.28 “Saját belátásod szerint, mennyire vagy tisztában a jó jelszóval kapcsolatos elvárásokkal?”
2.29 “Nagyon jók és biztonságosak a jelszavaim.”
2.30 “Az érzékenyebb, fontosabb adatokhoz hosszabb jelszót szoktam használni.”
2.31 “Figyelembe veszed-e új jelszó megadásánál, ha mutatja az adott alkalmazás a jelszó erősségét?”
2.32 “Mennyire jellemző, hogy törekszel az erős jelszóra?”

Ennek eredményeképpen az látható, hogy a közszférában 4,33-as átlagos értéket kaptam, míg az üzleti szférában ennél valamivel magasabb átlagos értéket 4,38-at kaptam az aggregált index értékre. Amelynél fontos kiemelnem, hogy mivel összesített indexről van szó, ezen eltérés is rendkívül jelentősen reprezentálja, hogy a közigazgatási érték alacsonyabb.

2.35 “Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?”



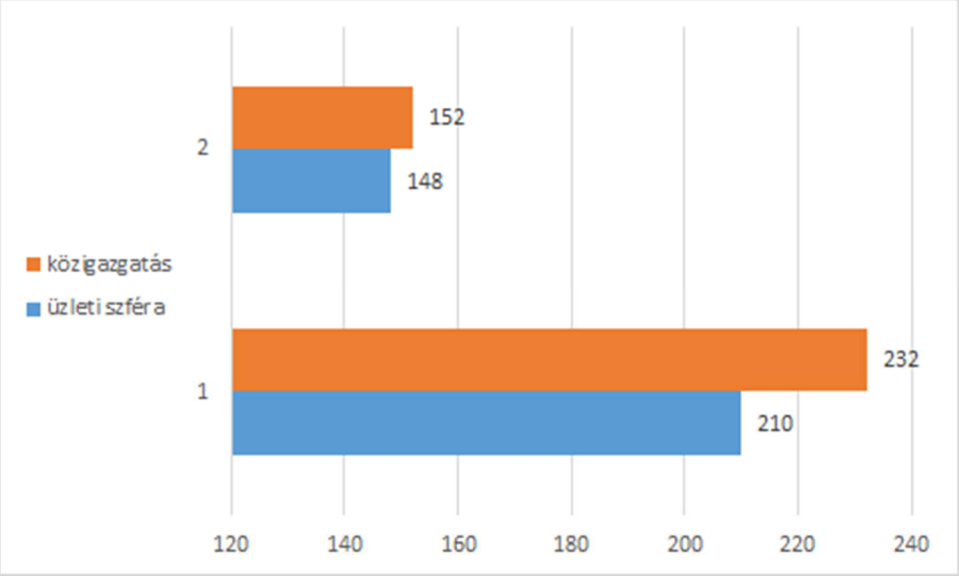
33. ábra: Oktatásban részesültek és nem részesültek eloszlása a közigazgatási mintán, forrás: saját szerkesztés

Igen 152
Nem 227
Nem válaszolt 5

Ugyanakkor az egyes szektorok összehasonlítása adott mintán belül
üzleti szféra 358 válaszadóból 148 fő kapott képzést,
közig szféra: 384 válaszadóból 152 fő kapott képzést, amely összességében adott mintán belül vizsgálva közel 5%-os átoktatottsági hiányt jelez a közigazgatáson belül az üzleti szférához

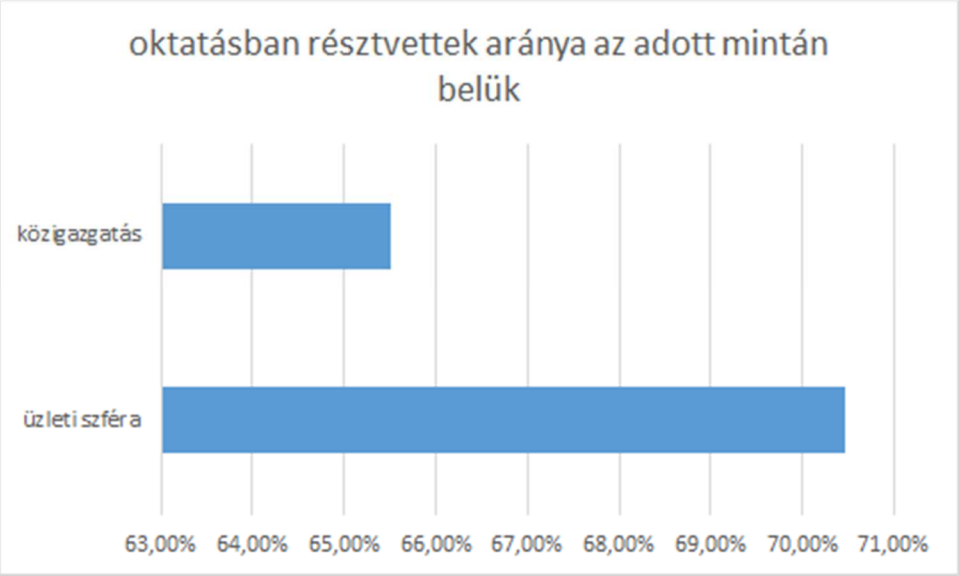
viszonyítva. Saját mintán belül ez az érték 34,48%-a a válaszadóknak azt mondta, hogy nem kapott ilyen képzést. Az egy külön vizsgálat tárgyát képezheti, hogy a közigazgatásban ahol előírt az oktatási kötelezettség, a válaszadók miért csak 40%-a válaszolta, hogy oktatásban részesült.

Az alábbi diagramon az egyes mintákon belüli átoktatottságot jelenítem meg:



34. ábra: Szféra szerinti csoportosításban az oktatásban részt vettek és nem oktatottak megoszlása, forrás: saját szerkesztés

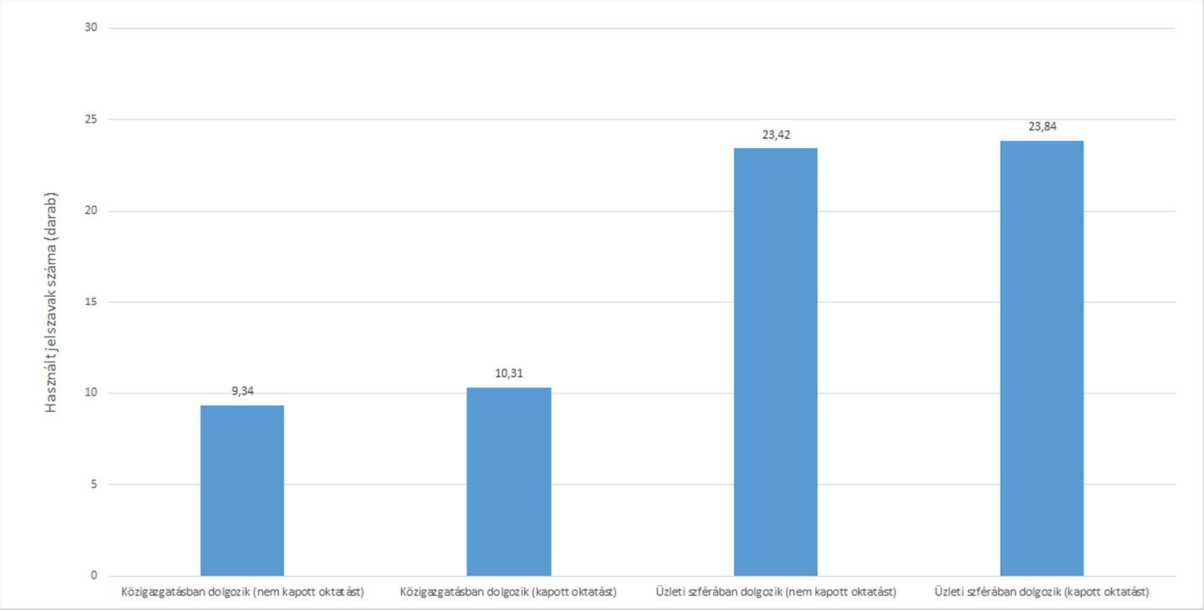
A mintán belüli százalékos eltérést talán még jobban vizualizálható, az alábbi ábra segítségével



35. ábra: Az oktatásban résztvevők aránya adott mintán belül vizsgálva százalékosan, forrás: saját szerkesztés

A kérdőívem segítségével több irányból is megközelítettem a kérdést, kivédve azt az esetleges hibát, amely a 2013-as (Illéssy, Nemeslaki, Som) kutatásomnál az interjús kérdések és a kérdőív kiértékelés során is lehetséges kockázatként értékeltem, azaz, hogy esetleg a válaszadó a kérdésnek akar megfelelni, tudása szerint próbál egy jobb választ adni, jobb színben feltűnni.
Ezért két másik jelszó minőségre vonatkozó blokkot más-más témában emeltem be a kérdőívre, az egyik az inkább a magánéletben használható jelszószéfre a másik pedig inkább a munkaszervezetekben használt jelszó élettartam, megváltoztatására vonatkozó kérdésblokkra fókuszált.

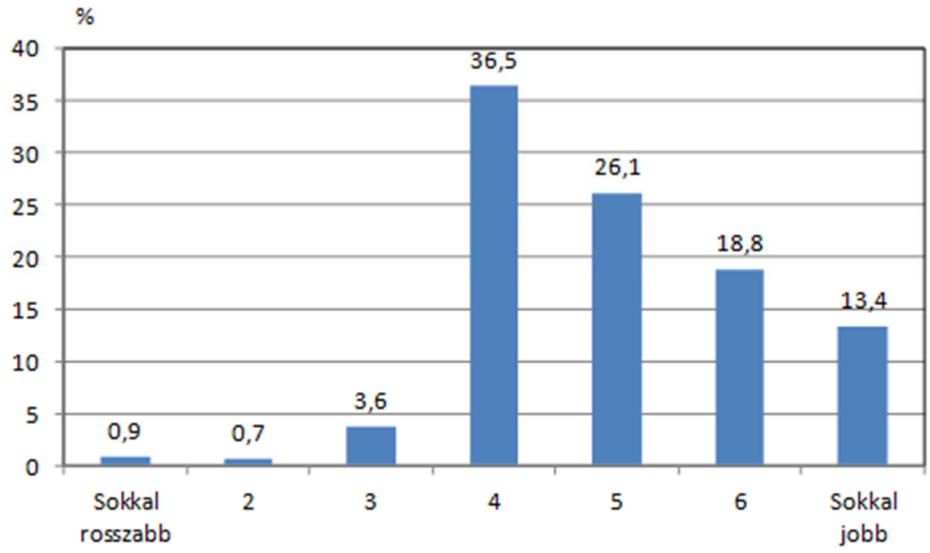
Kutatásomban vizsgáltam, hogy 2.1 "Hozzávetőlegesen hány darab különböző jelszót használsz?" kérdésre a közigazgatási mintán 9,34 az átlag. Ha a mintán belül csak azokat vizsgálom, akik közigatásban dolgoznak és oktatást kaptak, az átlag ekkor 10,31-re emelkedik.
Üzleti szférában vizsgálva az előbbieket a teljes mintán 23,42 az átlagos jelszódarabszám. Míg az üzleti szférában oktatást kapottak 23,84 az átlagos jelszó szám. Több, mint a duplája a közigazgatásban mérhető értéknek.



36. ábra: "Hány darab különböző jelszót használsz?", szféra és oktatás szerint ábrázolva, forrás: saját szerkesztés

A 36. számú ábrán a használt jelszavak hosszát ábrázoltam a szféra és oktatásban való részvétel függvényében.
2.45 "Véleményed szerint a Te jelszavaid jobbak vagy rosszabbak az ismerőseid által használtaknál?"
Általános, a teljes mintán tett megfigyelés, ahogy azt már disszertációmban kifejtettem kongruensen viselkednek, racionalizálják cselekedeteiket és belső hiedelemvilága konzekvens maradjon. Az emberek ennek megfelelően "legalább annyira" jónak tartják saját jelszavaikat, mint mások jelszavát, bár ugye magától értetődik, hogy jelentős része nem ismert. A válaszadók szinte

kivétel nélkül úgy gondolják, hogy a jelszavaik legalább olyan jók, mint másoké. Ebből nagyjából az következik, hogy akinek nem jó a jelszava, az nem is tud róla, hogy nem jó.



37. ábra: "Mit gondolsz más jelszaváról, a Tiéd rosszabb vagy jobb?" kérdésre adott válaszok (%) forrás: saját szerkesztés

A teljes mintán: 4,37 az átlag, teljes mintán oktatással: 4,57, közig mintán: 4,33, mig közig mintán oktatással: 4,5. Mind az oktatással, mind az a nélküli csoportban vizsgálva a közigazgatásból válaszadók értékei alacsonyabbak, amely szintén a lemaradást támasztja alá. Azaz bár eleve megmutatkozik a teljes mintán a személyek kongruens magatartásának és racionalizálásának mintázata. De ezen túlmutatóan az is látható az egyes számadatokból, hogy a közigazgatási mintán, mind az oktatottak, mind pedig a teljes mintán közigazgatási mintát tekintve alacsonyabbra értékelik a saját jelszavaikat jóságát, mint a üzleti szférában dolgozók.

Közigazgatási minta átlaga: 4,33

üzleti szféra minta átlaga: 4,84.

Tehát a saját jelszó jóság önértékelése is alacsonyabb a közigazgatási szektoron belül.

2.47-2.48 "Tudod-e valamelyik ismerősöd bármely jelszavát? Honnan tudod?"

A közigazgatási mintában vizsgálva a válaszadók 57,03% -a százaléka tudja mások jelszavát. Ezen belül 58,03% százalékában azért, mert a másik megadta.

38. ábra: "Tudod-e valamelyik ismerősöd jelszavát?" kérdésre adott válaszok (%) forrás: saját szerkesztés

Ha mélyebben, részleteiben érdemes vizsgálni a kérdést a jobb megértés és a gyökér okok kifejtése érdekében. A 38. számú ábráról leolvasható, az egyértelmű tény, hogy egy olyan általános gyakorlatra derült fény, amely jelenség és egyértelműen rossz gyakorlat. Alapjaiban degradálja az információbiztonsági elvárásokat.

Ezt az elméletet támasztja alá a következő kérdésre adott válaszok elemzése is, 2.48 "Honnan tudod az ismerősöd jelszavát? "Amely révén azt kívánom ismételten alátámasztani, hogy a felhasználókban megvan a szándék a szabálykövetésre, ha azt értik és képesek a munkafolyamataikkal összehangolni, ehhez a szükséges támogatást megkapják. Ugyanakkor ennél a kérdésnél kivontam azokat a válaszokat, ahol önként történt meg a jelszavakat átadása és csak kifejezetten azokat a válaszokat vizsgáltam, ahol a felhasználó tudta nélkül szerezte meg valahogy a jelszavát a válaszadó. A számok alapján a teljes mintán 7,4% mondta azt, hogy a felhasználó tudta nélkül szerezte meg a jelszót, a közigazgatásban ez a szám 2,28%. Ennek oka ismét abban található meg, hogy a szabályzatokban ismert retorziós politika is jelenthet némi visszatartó erőt.

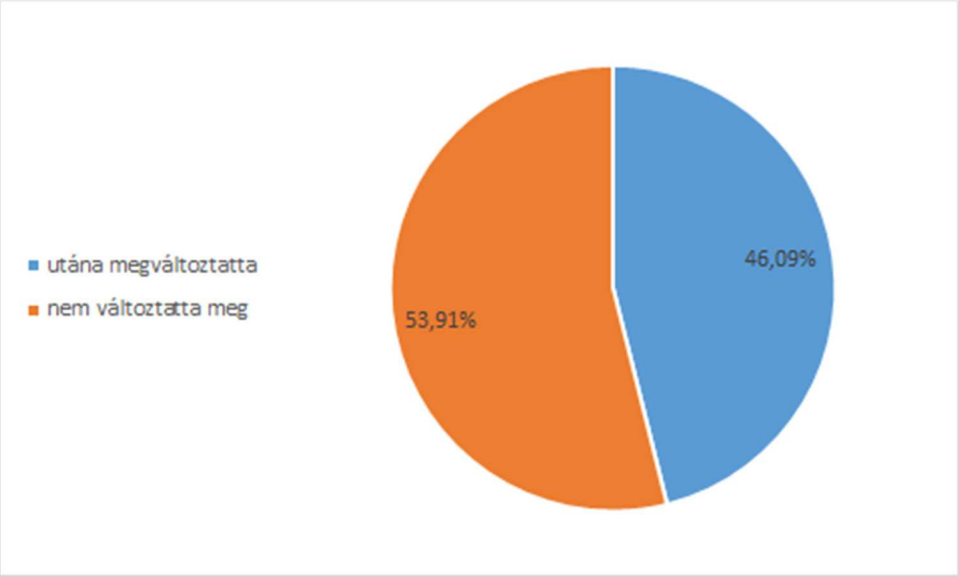
A teljes gondolati sík és gyakorlat megértéséhez kövessük végig a teljes folyamatot. Azt feltételezzük, hogy szabálykövetésre alkalmasak és arra törekszenek a felhasználók. Amennyiben ez így van, akkor ennek vissza kell köszönni a jelszó megadást követő mozzanaton is. A 2.43 "Ha ideiglenesen adtad meg másnak a jelszavadat bármilyen okból, az ok megszűnése után megváltoztattad-e azt?" kérdésre vizsgálom meg és értékelem ki a válaszokat.

A teljes mintán vizsgálva 797 válaszadó mondta, hogy 2.42 "Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?", ebből 554 fő választotta azt, hogy 2.43 "Ha ideiglenesen adtad meg másnak a jelszavadat bármilyen okból, az ok megszűnése után

megváltoztattad-e azt?" Érdekes jelenség, hogy 646 fő válaszolt erre igennel, ha nem tekintjük az előbbi szűkítést a 2.42.-es kérdésre. Amiből ismét az látszódik, hogy úgy tekintenek a rövid idejű jelszó megadásra, majd esetlegeses azt követő változtatására, mintha meg se történt volna, azaz racionalizálnak, hogy belső konguencia megmaradjon.

Közigazgatás: 219
Üzleti: 258

A közigazgatási mintán a 2.43 "Ha ideiglenesen adtad meg másnak a jelszavadat bármilyen okból, az ok megszűnése után megváltoztattad-e azt?" válaszok eloszlását az alábbi ábra mutatja.



39. ábra: "Ha ideiglenesen adtad meg másnak a jelszavadat bármilyen okból, az ok megszűnése után megváltoztattad-e azt?" kérdésre adott válaszok (%), forrás: saját szerkesztés

Az látható, a 39. számú ábrán, hogy közel fele-fele az eloszlás, 53,19% azt válaszolta, hogy nem változtatta meg. Amely révén voltaképpen a személyre kiadott azonosító jelszó párost más megismerhette és azzal később akár vissza is élhet a felhasználó nevében.
Kutatásaim során természetesen más modelleket is figyelembe vettem, így a TAM-t is, amely voltaképpen azt mondja, hogy a információs rendszer, a technológia elfogadása befolyásolja a biztonságtudatos magatartást, a szabálykövetési hajlandóságot.

A 3.1 "Hány éve használsz számítógépet?" kérdésre átlagosan 17 év a teljes mintában a válasz. Így megvizsgáltam, hogy 17 év, átlagos használati idő alatt mennyire jellemző a jelszó megosztás (2.42 "Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?") amire 460 fő válaszolt igennel, míg az átlag feletti

számítógéphasználati idővel rendelkezők körében ez a szám, jelentősen kisebb 309 fő eredményt adott.

A közig mintán a (2.42 "Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?") kérdésre a fenti megoszlás szerinti csoportosítást alkalmazva a 17 év, átlagos használati idő alatt 126 fő válaszolt igennel, míg az átlag feletti számítógép-használati idővel rendelkezők körében ez a szám, jelentősen kisebb 87 fő eredményt adott.

2.50 "Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?" kérdésre a teljes mintából 1113 fő válaszolt erre a kérdésre, melynek átlaga 3,28 egy 6 fokozatú skálán.

A közigazgatásban ez az érték 3,29, azaz magasabb, amely jelen esetben "rosszabb", mert valószínűbb, hogy az új jelszó köthető a régihez. Ami érdekes jelenség, hiszen arra enged következtetni, hogy valamilyen nehézség vagy tudáshiány állhat az egyértelmű biztonsági ajánlással szembe menő gyakorlat mögött. Ami viszont arra utal, hogy lemaradást tapasztalható a közigazgatási területen.

Ugyanakkor a TAM modellre hivatkozva ismét, a IKT-képességek is mérésre kerültek. Így a 3.4 Milyennek tartod a számítógépes alapismereteidet? kérdésekből indexet képeztem és az indexált válaszokat vizsgáltam. A 3.4 - 3.12-es kérdésig képzett indexet vizsgáltam.

Az üzleti szférában az indexált értékek átlaga: 56,606

Az üzleti szférában az indexált értékek átlaga, azok körében akik oktatást is kaptak: 59,831

Az közig szférában az indexált értékek átlaga: 48,158

Az közig szférában az indexált értékek átlaga, azok körében akik oktatást is kaptak: 50,302

Disszertációmnak nem témája az IKT-képességek és információbiztonsági tudatosság közötti vizsgálat, azonban látható, hogy a közigazgatásban az IKT képességek vonatkozásában kapott értékek alacsonyabbak, ez érvényes az oktatásban részesült csoportra is, valamint látszólag együtt mozog az információbiztonsági lemaradással is. Későbbi kutatásra érdemes lehet ennek pontosabb statisztikai vizsgálata.

A 2.36 "Kérlek, fejtsd ki a jelszavakkal, oktatással, biztonsággal kapcsolatos véleményedet pár mondatban!" szabadszöveges kérdésre, - az összes válaszadó közül - meglepően sok, 453 kitöltő írt hosszabb - rövidebb választ. Már a kérdőív kidolgozásakor feltett szándékom volt, hogy megvizsgáljam mit lehetséges kimutatni a szóhasználati elemzésből. Egyrészt tudományos szempontból is roppant érdekelt, másrészt eddigi megfigyeléseim és diverzifikált korosztályoknak tartott tudatossági előadásaim során is megfigyeltem tipizálható szó és mondatfordulatokat, amelyeket bizonyos attitűdhöz lehetett kapcsolni. A kérdés ezen kérdésére adott válaszok kiértékelése azonban rendkívül sok utómunkát igényelt annak érdekében, hogy az

egyes szavak számos ragozott alakja ne külön-külön szóként jelenjen meg a szófelhőben vagy elemzésben, hanem valamilyen halmazt, csoportot alkotva. Ide tartozik még a ragozott alakokon kívül a helytelen helyesírással írt szavak, az ékezet nélküli karakterekkel írt szavak, rövidítések, valamint a kis és nagybetű különbözőségekből fakadó eltérések is.

Ezen tisztítását követően a kötőszavak és ragok, ékezetes karakterek cseréje után a negyedik leggyakoribb szó az oktatás lett. Természetesen jól mutatja a jelszó kezelés problémáját a többi szó is, a megjegyezhetőség, stb. A témához triviálisan kapcsolódó szavak (jelszó, használ, biztonság) elhagyásával mindenképpen élre tör a válaszadások alapján az oktatás, annak igénye.

40. ábra: "Kérlek fejtsd ki a jelszavakkal, oktatással, biztonsággal kapcsolatos véleményedet" kérésre adott szabad szavas válaszokból képzett szófelhő. Forrás: Saját szerkesztés.

A 40. számú ábrán a gyakoriság függvényében változott egyes szavak betűmérete. A gyakoribb szavak nagyobb betűmérettel rendelkeznek.

Az üzleti és közigazgatási szféra komplexebb összehasonlítása érdekében statisztikai próbákat végeztem. A beérkező adatok feldolgozásához az IBM SPSS statisztikai programcsomagját alkalmaztam.

Első lépésben azt vizsgáltam meg, hogy a következő négy kérdésre adott válaszok mennyire térnek el az üzleti és közigazgatási szféra esetében:

- Hozzávetőlegesen hány darab különböző jelszót használsz?
- Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?
- Hány karakter a leghosszabb jelszavad?

- Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?

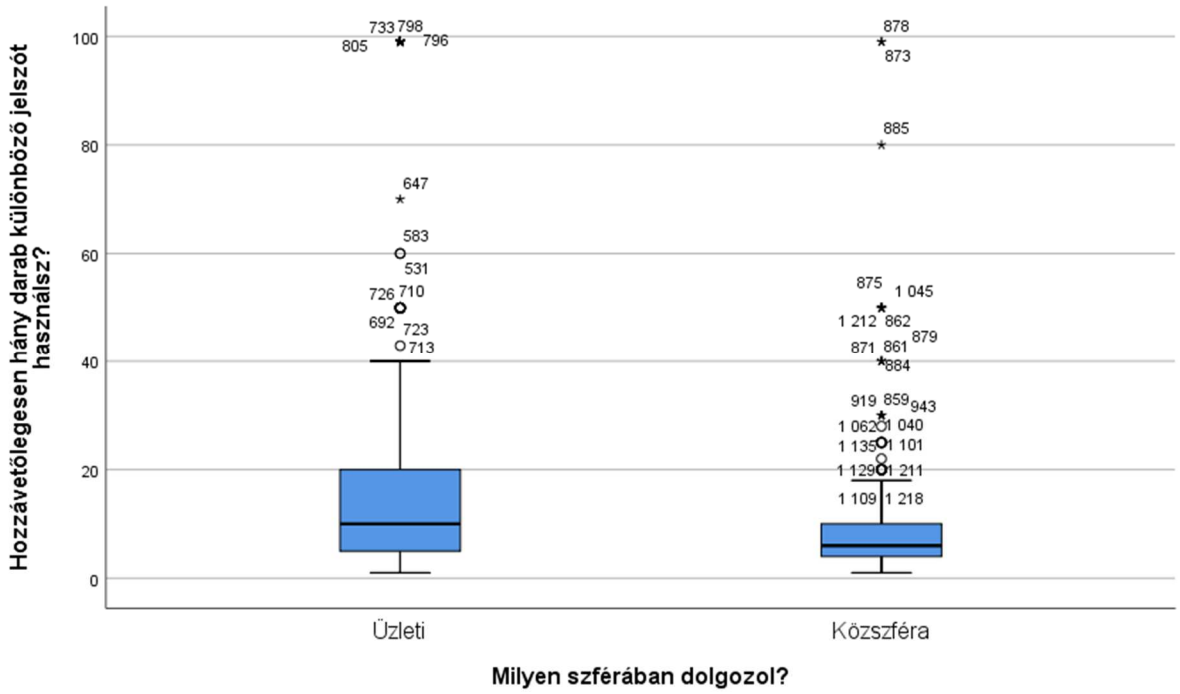
A Kolmogorov-Smirnov próba szignifikáns eredménye ($p<0.001$) alapján nem igazolható az adatok normális eloszlása csoportonként, így a kétmintás t-próba helyett a Mann-Whitney nemparaméteres próba alkalmazása mellett döntöttem a két csoport (üzleti, közszféra) közötti esetleges eltérések vizsgálatakor a mennyiségi és sorrendi változók esetében.

	Hozzávetőlegesen hány darab különböző jelszót használsz?	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Hány karakter a leghosszabb jelszavad?	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, elégé hasonlít a régi jelszóhoz?
Mann-Whitney U	49119,500	49354,500	64898,500	36343,500	41138,000	58861,000
Wilcoxon W	124585,500	123659,500	140364,500	110648,500	106841,000	116831,000
Z	-6,739	-6,504	-1,256	-10,929	-7,371	-2,316
Asymp. Sig. (2-tailed)	0,000	0,000	0,209	0,000	0,000	0,021

9. táblázat: Mann-Whitney próba eredménye, forrás: saját szerkesztés:

A Mann-Whitney próba szignifikáns eredménye ($p<0.05$) alapján jelentős eltérés igazolható az üzleti és közszféra dolgozói között az információbiztonság-tudatosságban. Ugyanis a hat vizsgált kérdés esetében csak a jelszó változtatásának sűrűségében nem igazolható jelentős különbség ($Z=-1.256$, $p=0.209$). Az üzleti szférában jelentősen több és hosszabb jelszót használnak a közszférához képest, valamint itt kevésbé jellemző, hogy az új jelszó hasonlít a régihez.

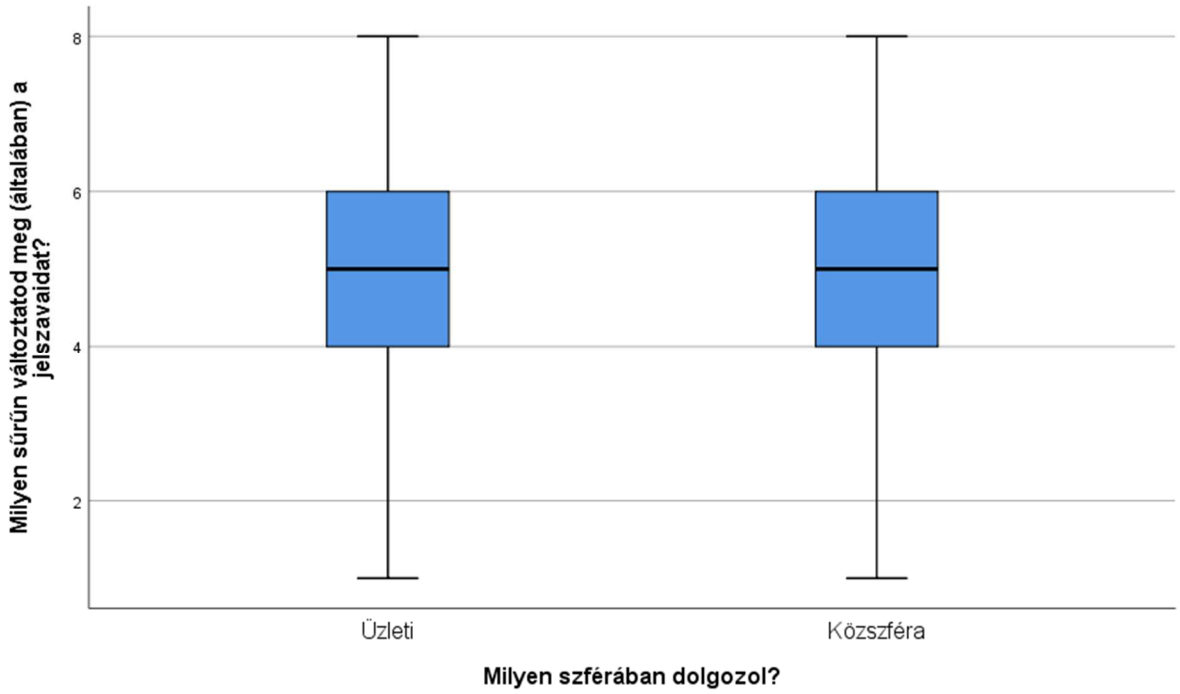
Ezt követően elkészítettem a boxplot ábrát a kimutatás szemléltetéséhez.



41. ábra: "Hozzávetőlegesen hány különböző jelszót használsz?" kérdésre adott válaszok box-plot ábrája szféránként, forrás: saját szerkesztés:

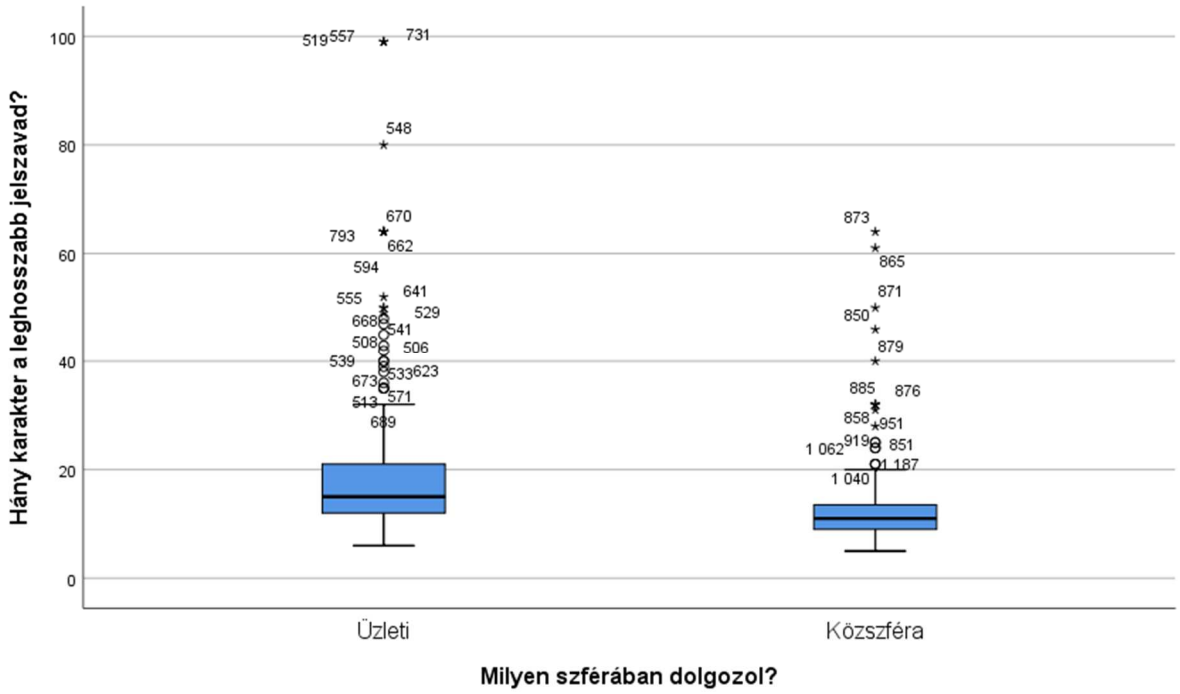
A 41. számú ábrán boxplot kimutatásban látható a két szféra. A boxpoltok jól szemléltetik a két szféra közötti eltéréseket. Az üzleti szférában több különböző jelszót használnak. Amely így alátámasztja a hipotézisem, hogy a közigazgatási szférában lemaradás tapasztalható.

A "Milyen sűrűn változtatod meg (általában) a jelszavaidat?" kérdésre adott válaszok boxpolt elemzését elkészítettem és az alábbi 42. ábrán látható a szféra szerinti eloszlása.



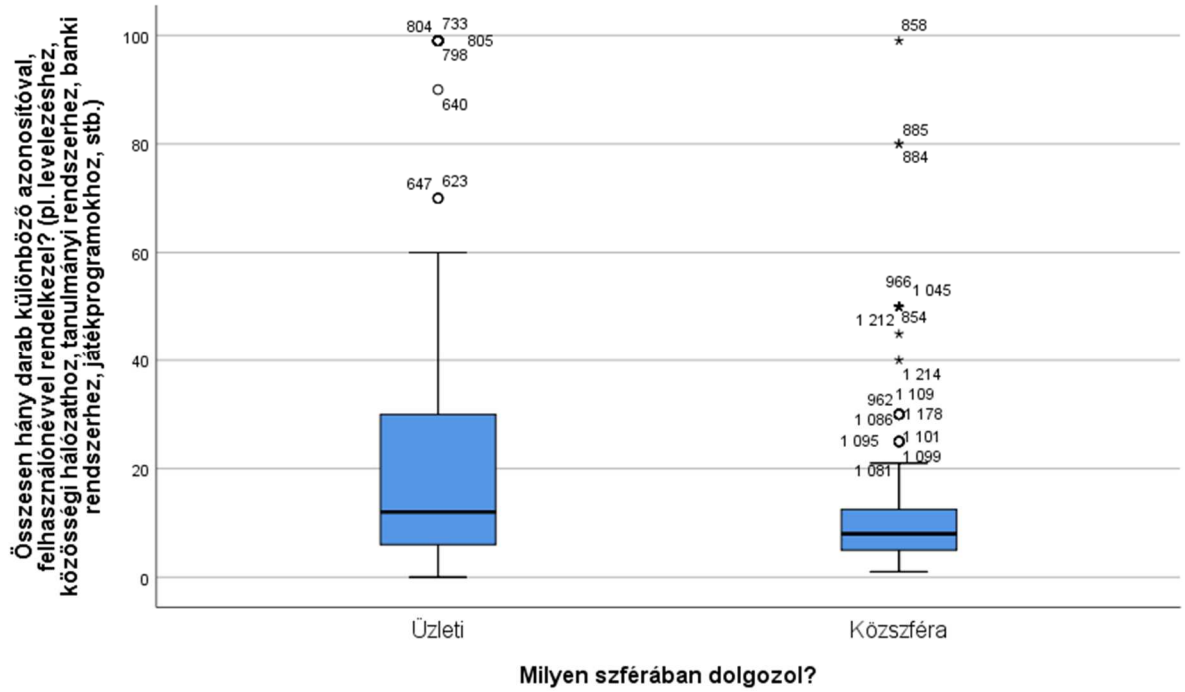
42. ábra: "Milyen sűrűn változtatod meg (általában) a jelszavaidat?" kérdésre adott válaszok boxpolt ábrája szféránként, forrás: saját szerkesztés

A "Hány karakter a leghosszabb jelszavad?" kérdésre adott válaszok boxpolt elemzését elkészítettem és az alábbi 43. ábrán látható a szféra szerinti eloszlása.



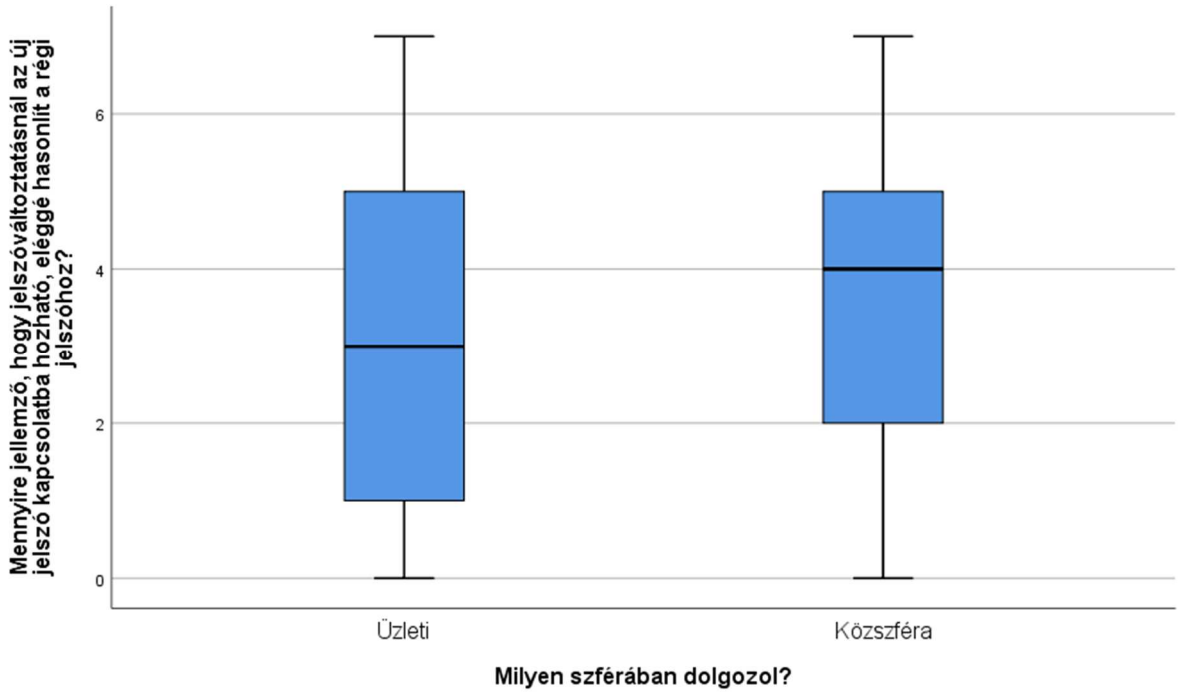
43. ábra: Hány karakter a leghosszabb jelszavad? kérdésre adott válaszok boxpolt ábrája szféránként. Forrás: Saját szerkesztés.

A Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? kérdésre adott válaszok boxpolt elemzését elkészítettem és az alábbi 44. számú ábrán látható a szféra szerinti eloszlása.



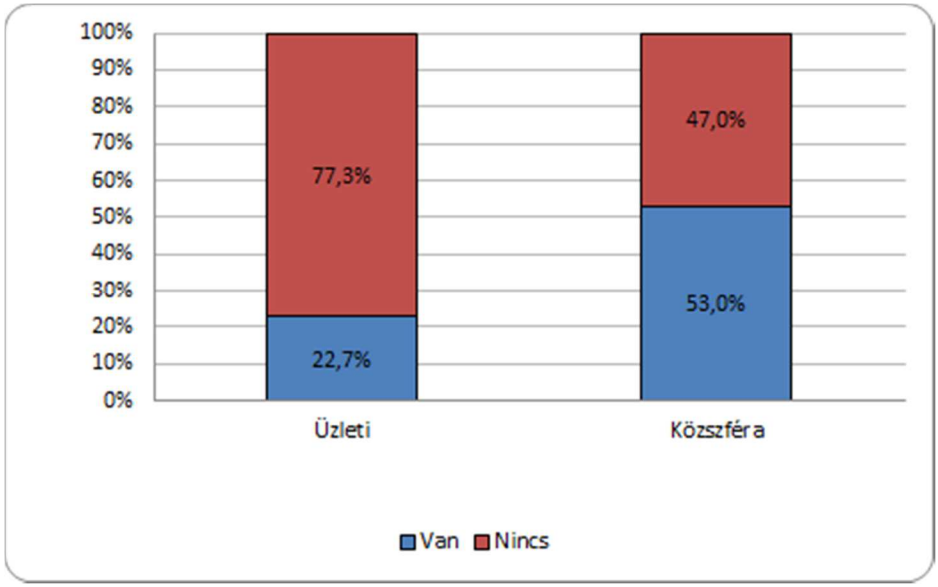
44. ábra: "Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?" kérdésre adott válaszok boxpolt ábrája szféránként, forrás: saját szerkesztés

A Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz? kérdésre adott válaszok boxpolt elemzését elkészítettem és az alább 45. ábrán látható a szféra szerinti eloszlása.



45. ábra: "Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?" kérdésre adott válaszok boxpolt ábrája szféránként forrás: saját szerkesztés

A jelszóképzés fontosságáról és lehetséges indikátor szerepéről már beszámoltam, így a "Van-e olyan jelszavad, ami tartalmaz személynevet?" kérdésre adott válaszok elemzését elkészítettem és az alább 46. számú ábrán látható a szféra szerinti eloszlásban.

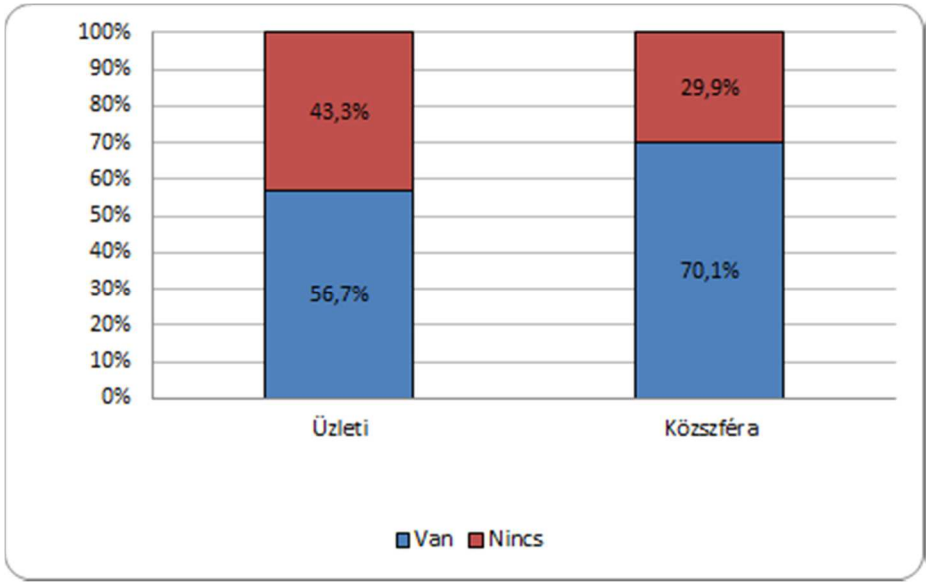


46. ábra: "Van-e olyan jelszavad, ami tartalmaz személynevet?" kérdésre adott válaszok szféránkénti megoszlása (%), forrás: saját szerkesztés

A 46. számú ábrán, annak függőleges tengelyén a százalékos értékek kerültek feltüntetésre. Kék színnel az igenleges válaszok, míg piros színnel a nemleges válaszok kerültek ábrázolásra, szféránként.

Ezen kívül a khi-négyzet próba szignifikáns eredménye (Chi2=69.456, df=1, p<0.001) alapján jelentős eltérés igazolható az üzleti és közszféra között a személynevet tartalmazó jelszó előfordulási arányában: a közszférában dolgozók jelentősen nagyobb arányban rendelkeznek ilyen jelszavakkal. Amely egyrészt alátámasztja hipotézisem, másrészt arra utal, hogy a szabálytudás, vagy szabály alkalmazás gyakorlata elmarad.

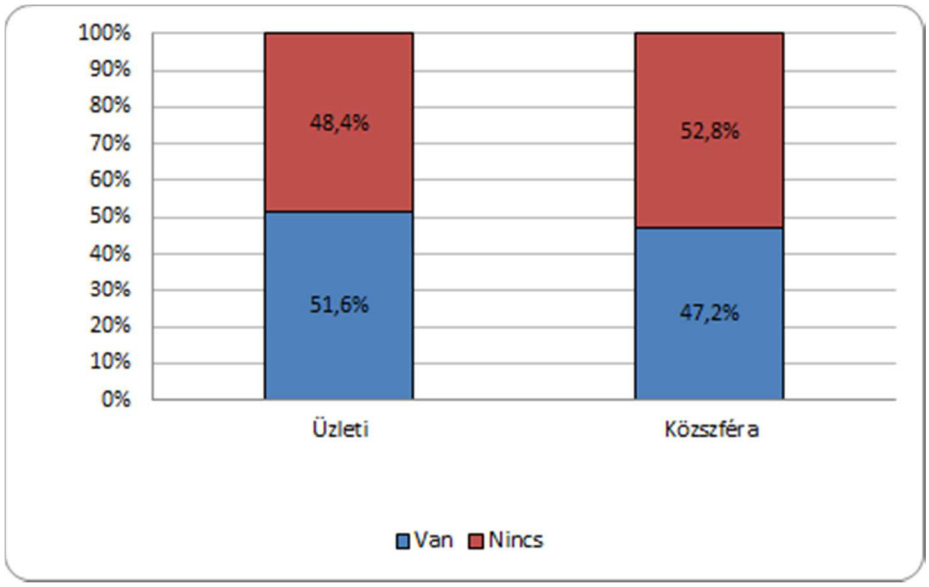
A Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul? kérdésre adott válaszok elemzését az alábbi ábra szemlélteti:



47. ábra: "Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?" kérdésre adott válaszok szféránként (%) forrás: saját szerkesztés

A 47. számú ábrán, annak függőleges tengelyén a százalékos értékek kerültek feltüntetésre. Leolvasható, hogy a közszférában dolgozó válaszadók magasabb értékbe adták azt a válasz, hogy valamilyen név, értelmes kifejezés van a jelszavukban.
A változókon elvégeztem a khi-négyzet próbát, amelynek szignifikáns eredménye (Chi2=13.534, df=1, p<0.001) alapján jelentős eltérés igazolható az üzleti és közszféra között abban, van-e olyan szó, név, kifejezés, amelyik több jelszóban is előfordul: a közszférában dolgozók jelentősen nagyobb arányban rendelkeznek ilyen jelszavakkal.

Érdekes megfigyelésre jutottam ugyanakkor a Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok? kérdésre adott válaszok elemzése során.



48. ábra: "Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?" kérdésre adott válaszok szféránként (%), forrás: saját szerkesztés

Bár az 48. számú ábrán leolvasható és első pillantásra látszik különbség, de a khi-négyzet próba eredménye (Chi2=1.389, df=1, p=0.239) alapján nincs jelentős különbség az üzleti és közszféra között abban, van-e olyan jelszó, amit más is tud.

4.1.2 KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI KÉRDŐÍV ELEMZÉSE

Ha a globális képet tekintjük, akkor megállapíthatjuk, hogy a válaszolók jól teljesítettek, hiszen 87%-uk a második legalacsonyabb kockázati besorolású csoportba került, mindössze 13% teljesített ennél rosszabbul és ők sem kaptak közepesnél gyengébb osztályzatot. Figyelembe kell azonban venni a minta torzító hatásait, a budapestiek nagyobb arányát, ők feltehetően eleve nagyobb tudatossággal rendelkeznek, és munkahelyeik esetében is nagyobb eséllyel feltételezhető, hogy gondot fordítanak az elektronikus információbiztonsági szabályok betartására.

Érdekes, hogy a válaszadók életkori szerinti megoszlása alapján nem lelhetők fel lényeges különbségek, a teljes mintában hasonló arányban fordulnak elő jó értékeléssel rendelkezők a különböző korosztályokban. A közepes kockázati osztályba sorolt válaszadók életkor szerinti vizsgálatakor azonban kitűnik, hogy kevesebb 35 év alatti, illetve 45 és 54 év közötti személy fordul elő itt, mint a teljes mintában. Azonban a középgenerációnak tekintett 35-44 éves korosztály nagyobb arányban fordul elő az adott osztályban, mint a teljes mintában (43% vs. 36%). Az alacsony elemszám miatt azonban nem feltétlenül tekinthető a minta reprezentatívnak. (Illéssy, Nemeslaki, Som, 2014)

A kérdéseket három nagyobb kategóriába soroltuk, hogy részletesebb képet alkothassunk azokról a területekről, ahol jól, illetve rosszabbul teljesítenek a válaszadók. A szervezeti dimenzió a céges szokások és eljárások mérésével kapcsolatos kérdéseket tartalmazza (IB-részleg jelenléte, a számítógép feltörésére adott reakció, a céges adatok másolásának, hazavitelének kérdése, IB-képzés stb.) A kérdések egyéni dimenziója általános felhasználói ismeretekre és szokásokra vonatkozik (a gép feltörésének észlelése, céges jelszó kiadása, levelek csatolmányainak megnyitása stb.). A kérdések infrastrukturális dimenziója azt vizsgálja, hogy a válaszadók mennyire tekintik biztonságosnak a munkahelyi rendszereket (vírusirtó, automatikus frissítések, vírus vagy trójai program előfordulása a céges gépen).

	Globális	**Szervezeti**	**Egyéni**	**Infrastrukturális**
		dimenzió		
Jeles	0%	7%	0%	67,5%
Jó	87%	92%	77%	29%
Közepes	13%	1%	23%	3,5%
Összesen	**100%**	**100%**	**100%**	**100%**

10. táblázat: Az IB-tudatosság szintje globálisan és a mért dimenziók szerint, forrás: Illéssy, Nemeslaki, Som, 2014

Mint a táblázat adataiból látható, az infrastrukturális dimenzióméró válaszok értékei haladják meg legjelentősebb mértékben a globális képet: 67,5%-uk az e dimenziókra számított értékek szerint „jelesre vizsgázott", további közel 30% ért el jó eredményt és mindössze 3,5%-uk kapott közepes kockázati besorolást. Itt újra fel kell hívnunk a figyelmet arra a torzító hatásra, amelyet a budapestiek túlsúlya jelentett a mintán belül. További kritikus észrevételeket is teszünk még az átfogó értékelés után, melynek során a válaszok belső ellentmondásait elemezzük.

	Jó osztályzat	**Közepes osztályzat**	**Átlag a mintán belül**
Életkor szerint			
35 év alattiak	34,5%	21,5%	31,5%
35-44 év között	34%	43%	36%

45-54 év között	23%	24,5%	23%
55 év felettiek	8,5%	11%	9%
Nem			
Nő	57%	46%	54,5%
Férfi	43%	54%	45,5%

11. táblázat: Az egyéni dimenzió értékei életkor és nem szerint, forrás: Illéssy, Nemeslaki, Som 2014

A 11. számú táblázatban az látható, hogy jó és közepes kategóriában, illetve ehhez viszonyítottan a teljes mintán belül milyen a válaszadók életkor, illetve nem szerinti megoszlása. Soronként leolvashatóak a mintaátlaghoz viszonyított eltérések. Az összevetés alapján igazolást nyer az a korábbi megállapítás, hogy habár az életkort tekintve a legfiatalabb korosztály teljesítménye a legjobb, azonban a 35-44 éves középkorosztály a teljes mintában képviselt arányukhoz képest nagyobb arányban teljesít rosszul, mint a náluk fiatalabbak vagy idősebbek. Az is kiderül, hogy az értékek nemek szerint is eltérőek. A nők aránya 10%-kal kisebb a közepes osztályzatot kapott csoportban, mint a minta egészében, ám a férfiak esetében ennek ellenkezője érvényesül, a teljes mintában képviselt arányukhoz képest számottevően többen fordulnak elő a közepesre értékel válaszadók között.

Kérdőíves felmérések esetén megvan annak az esélye, hogy a felmérésnek való megfelelési szándék hatással van a válaszadásra. Fontos arra is tekintettel lenni, hogy a kérdőív online felületen való kitöltése csak a rendszeresen számítógéppel dolgozók, illetve az informatikai eszközökhöz pozitívan viszonyulók esetében természetes elvárás. Mindezt figyelembe véve a kitöltés során tapasztaltakról elmondhatjuk, hogy a válaszadáskor kihagyott kérdések száma monoton növekvő tendenciájú. Minél később fordul elő egy kérdés a kérdőívben, annál nagyobb arányban hagyják megválaszolatlanul a megkérdezettek.

A felmérés szerint a válaszadók 88% esetében rendelkezik a munkahelyük informatikai biztonsággal foglalkozó részleggel.

- Ebből kifolyólag a megkérdezettek 12% esetében olyan munkahelyről van szó, ahol nincs jelen IB-részleg, ami valószínűsíti jelentős informatikai biztonsági problémák fennállását. A részleg hiányában felső vezetés nem alkothat reális képet az elektronikus információs és informatikai biztonságról. Hiányzik az alkalmazottak ezirányú képzése és felvilágosítása is. Sem a felső vezetés, sem az üzemeltetés nem kap visszajelzést az üzemeltetés feladatvégzéséről.

• A másik csoport magas arányszáma (88%) azonban mindenképp pozitívnak mondható, és indokolja további kérdések felvetését.

- 8% nem érzi biztonságosnak a számítógépét adatlopásokkal szemben.
- 14%-a a válaszadóknak talált már trójai programot a gépén munkavégzés közben.
- 25% inkább úgy gondolja, hogy csak az IT-részleg feladata a biztonság garantálása.
- 26%-a azt mondja, hogy megadta már másnak munkahelyi jelszavát.
- 33% nem tudja miről ismerhető fel valamilyen kéretlen (spam) levél
- 40%-a állítja, hogy nem venné észre, ha feltörnék a számítógépét.
- 49% pedig mindezek ellenére úgy gondolja, hogy megfelelően elegendő informatikai biztonsági képzésben részesül. Hozzászámolva a bizonytalanokat ez az arány 61%-ra növekszik.

Összegezve az látható, hogy magasnak és jónak tűnő számmal számos ellentétes információ azt a látszatot kelti, hogy ahol van és valóban létezik is ilyen egység; ott is kérdéses a működésének hatásfoka. Az a hatásfok, amely a felhasználók egyenszilárdságán és információ, informatikai biztonságán mérhető le. Különösen nagy gondnak látszik az, hogy a válaszadók 61%-a úgy gondolja, hogy megfelelően képzett. (Illésy, Nemeslaki, Som, 2014)

Az 1. 01. Van-e informatikai-biztonsággal foglalkozó részleg az ön munkahelyén? kérdésre igen: n=288 (88.07%) és nem: n=39 (11.93%) kaptunk. Ebből két következtetést lehet levonni, voltak olyan munkavállalók akik nem tudták, hogy van-e ilyen szervezeti egység a munkaszervezetben, vagy úgy gondolták, hogy legjobb tudomásuk szerint nincs ilyen. Ez természetesen a személyes interjúk során feltett kérdések és arra kapott válaszokból is vált érthetővé. Ebből viszont az is következik, hogy az a közel 12% munkavállaló minden bizonnyal nem kapott és nem is kaphatott információbiztonsági otkatást, ha ilyen szervezeti egység nincs a munkaszervezetükben.

A 02. Tudja-e, kihez kell fordulnia abban az esetben, ha számítógépét feltörték vagy megfertőződött, vírusos? kérdésre

igen: n=314 (96.91%)

nem: n=10 (3.09%) válaszok érkeztek. Ennek jelentése, hogy a felhasználók számára nem különül el sok esetben élesen az informatikai és információbiztonsági szervezeti egység, feladatkör vagy szabályzat. Ez az állítás köszön vissza a TAM modellnél is, és az IKT-képességekkel kapcsolatos értékek is ezt igazolják.

A 03. “Talált-e már valaha trójai programot vagy vírust a gépén munka közben?” kérdésre adott válasz megmutatja, hogy a felhasználók köze 15%-a találkozott már valamilyen vírussal, kártékony kóddal a saját munkafolyamatai során.

igen: n=46 (14.37%)

nem: n=274 (85.62%)

Tehát a téma és kérdés, a vizsgálatok jogosságát igazolja, hogy erősen kitett szektorról beszélünk.

A 04. “Ön szerint észrevenné-e, ha számítógépét feltörnék vagy megfertőződne?” kérdésre adott válaszok azt mutatják, hogy a felhasználók azt feltételezik, hogy a valamilyen módon azonnali vizuális, észlelhető hatása van annak, ha a számítógépük, információs rendszereik kompromittálódnak.

igen: n=190 (59.75%)

nem: n=128 (40.25%)

A médiában kapott információk, illetve a 2018-2021 itervallumban hatalmas méreteket öltött ransomware támadások pedig tovább erősítették ezt a hiedelmet. A valóság számos meg nem nevezhető Magyarországi és nemzetközi nagyvállalati példa alapján, de az interneten elérhető, nyilvánosságra került esetek, például: Hydro, EGIS stb. is azt mutatják, hogy ezen támadások akár a látványos jelek előtt 3-5 hónappal megelőzően kezdődik. Tehát nem biztos, hogy látványos eseményekkel társul. Éppen ezért fontos a biztonságtudatos magatartás, hogy a jelentési kötelezettségből adódó felelősség legyen a rutin része.

A 05. “Megadta-e már céges jelszavát másnak, akár cégen belül, akár cégen kívül?” kérdésre adott válaszok megalapozták a 2015-ös jelszóhasználat, mint indikátorra vonatkozó kutatásom során kialakított kérdőívet is olyan módon, hogy a kérdéskört ott is megjelenítettem.

igen: n=83 (26.18%)

nem: n=234 (73.82%)

Az itt kapott értékek tisztán közigazgatásból vett számok, a 2015-ös kutatásnál a kérdést kitöltő (közigazgatásban dolgozó) 367 válaszadó közül 174, azaz 47,41% válaszolt igennel, hogy “Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?” kérdésre. Ez alátámasztja, hogy általános jelenséggel van dolgunk.

Ide kívánkozik a 18. “Kérte-e már el az ön jelszavát a főnöke vagy valamelyik munkatársa?” kérdés, amely tovább árnyalja, jobban érthetővé teszik a kérdést, illetve okokat.

1. igen: n=90 (30.30%)

2. nem: n=207 (69.70%)

Tehát nem csak önkéntes vagy önkényes megoldásról van szó, hanem vélhetőleg a munkafolyamatok nem megfelelő kialakítása felmérése, a szabályzatok kialakítása során figyelembe nem vett tényezők együttesen vezetnek ilyen gyakorlatokhoz.

Fontos azt is látni, így meg kívánom mutatni, hogyan vélekednek a felhasználók a felelősség kérdéséről, így a 8.1 "A munkahelyem adatainak és infrastruktúrájának a védelme kizárólag az IT-biztonsági részleg feladata." kérdésre adott válaszokat tekintve:

1. - teljes mértékben egyetértek: n=14 (4.62%)
2. - egyetértek: n=44 (14.52%)
3. - nem tudom: n=18 (5.94%)
4. - nem értek egyet: n=165 (54.46%)
5. - teljes mértékben nem értek egyet: n=62 (20.46%)

azaz 19,14%, a bizonytalanokkal együtt pedig jelentős 25,08% azt gondolja, hogy nem elsősorban az ő felelőssége a védelem, hanem a szervezeti hatáskör.

A 8.2 "Nem részesülünk elég képzésben arról, hogyan védhetnénk meg cégünk számítógépeit és adatait." kérdésre adott válaszok azt támasztják alá, hogy a felhasználók jelentős része alapvetően nyitott attitűddel és a szabályzatnak megfelelni szándékoznak.

1. 1 - teljes mértékben egyetértek: n=26 (8.58%)
2. 2 - egyetértek: n=92 (30.36%)
3. 3 - nem tudom: n=36 (11.88%)
4. 4 - nem értek egyet: n=118 (38.94%)
5. 5 - teljes mértékben nem értek egyet: n=31 (10.23%)

Azaz nyitottak az oktatásra képzésre, ugyanakkor ez nem a szabályzatok olvasását jelenti, tehát az önállóan elsajátítható ismeretekre kisebb a nyitottság a személyes interjús tapasztalatok alapján, hogy önállóan próbálja megtalálni és megérteni a technikai leírásokat, azokat értelmezni a saját munkafolyamataira.

Disszertációmban többször rámutattam, hogy a személy magánéleti információbiztonsági és a munkaszervezetben tanúsított információbiztonsági viselkedése kongruens kell, hogy maradjon. Így a 16. "Használhatja ön saját mobil infokommunikációs eszközeit (pl. okos telefon) céges információk tárolására és átvitelére?" kérdés kapcsán kapott válaszok

1. igen, használhatom: n=52 (17.39%)
2. nem, nem használhatom: n=128 (42.81%)
3. igen, de csak a cég által nyújtott szolgáltatás igénybe vételével: n=63 (21.07%)
4. nem tudom: n=56 (18.73%)

azt mutatják, hogy a kérdés rendkívül fontos, hiszen 17,39% használja, azaz ezen adatok akár keveredhetnek, így magán eszközökön is ugyanolyan egyenszilárdság és védelmi megfontolásokat kell(ene), hogy érvényesüljenek, mint a céges eszközök esetében. Ez tovább erősíti, ill. a százalékot növeli a bizonytalanok, esetlegesen, alkalomszerűen használók köre további 18,73%-al. Valamint további 21,07% akiknek kifejezetten biztosít magáneszközön keresztül (BYOD) valamilyen szolgáltatás elérését a munkaszervezet. Ez így összességében 57,19%.

17. "Töltött le és telepített ön már szoftvereket, akár a munkájához kapcsolódóan (pl. PDF-konvertálás vagy képek átméretezése), akár személyes használatra (pl. zenehallgatás) a munkahelyi számítógépén?" kérdés azt sugallja, hogy az adott munkaszervezetben az IT rendszerben a felhasználóknak van valamilyen kimelet jogosultsága, amellyel a saját gépén képes lehet akár tetszőleges program telepítésére, valamint a kimelt jogosultság révén a számítógépe jogosultság eszkalációnak vagy egyéb kockázatoknak is jobban ki van téve.

A 20. "Milyen gyakran fordul elő, hogy céges adatokat kell lemásolnia és hazavinnie annak érdekében, hogy otthon tudjon vele dolgozni?" kérdésre adott válaszok:

1. majdnem mindennap: n=11 (3.72%)
2. legalább hetente egyszer: n=42 (14.19%)
3. legalább havonta egyszer: n=66 (22.30%)
4. soha: n=177 (59.80%)

két további dolgot is alátámasztanak. Egyrészt rendkívül fontos a nem csak a szigorúan cégen belül vett információbiztonsági előírások és szokások fejlesztése, hiszen a számítógép, adathordozó, maga az adat is kikerül(het) telephelyen kívülre. Másrészt nagyjából 40% érintett a válaszadók közül a telephelyen kívüli munkavégzésben. Amelyhez egy speciális adalékként a nem kizárólag a munkaszervezet által biztosított számítógépen keresztüli munkavégzés további kockázatokat jelenthet, a 21." Jelentkezett-e már be a céges informatikai rendszerbe valamilyen nyilvános számítógépről (pl. könyvtárban, hotelben, kávézóban)?" kérdésben ezt vizsgálva, a munkavállalók közel 5-ét érinti a kérdés:

1. igen: n=59 (19.93%)
2. nem: n=237 (80.07%)

Vizsgálataim során több kérdésnél is felmerült bennem a kérdés, hogy vajon ezen kockázatok, az adott felhasználói csoportok homogén módon, egymást részben átfedve, vagy pedig halmozotton kockázatot jelentő csoportokat képvilselnek-e.

Jelen esetben a 20. “Milyen gyakran fordul elő, hogy céges adatokat kell lemásolnia és hazavinnie annak érdekében, hogy otthon tudjon vele dolgozni?” kérdésre pozitív választ adott 40,21% közül 29,41% azaz a teljes minta 9,21%-a egybeesik a 21. “Jelentkezett-e már be a céges informatikai rendszerbe valamilyen nyilvános számítógépről (pl. könyvtárban, hotelben, kávézóban)?” kérdésre igen választ adókkal.

A 22. “Ön általában milyen gyakran változtatja meg jelszavát?” kérdésre adott válaszok azt támasztják alá, hogy szükséges emlékeztetni a munkavállalókat a kötelező, javasolt tevékenységre.

1. naponta: n=2 (0.68%)
2. hetente: n=0 (0.00%)
3. havonta: n=55 (18.58%)
4. félévente: n=15 (5.07%)
5. évente: n=4 (1.35%)
6. soha: n=8 (2.70%)
7. “A céges rendszer automatikusan figyelmeztet a lejárat előtt, és akkor változtatom meg.”: n=212 (71.62%)

Jó állam jelentés 2018 tartalmazza, hogy “a közigazgatásban kiemelkedően magas a női dolgozók aránya, és csupán minden negyedik beosztott tisztviselő férfi”, így a nemek arányát reprezentatívnak fogadtam el a válaszadók kapcsán.

4.1.3 KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI INTERJÚK ELEMZÉSE

A megkérdezett szakértők többsége a magyar IB-szabályozás nemzetközileg is élenjáró színvonalú, egyes vélemények szerint jóval előrébb tart, mint azt az informatikai infrastruktúra használatának fejlettsége indokolná. A stratégia, a törvény és a végrehajtási rendeletek logikusan épülnek egymásra, ezek elfogadását széleskörű egyeztetés előzte meg a szakmán belül. Mindez azonban nem feledtetheti el, hogy Magyarország nagy lemaradásból indult ezen a téren. Mivel a megkérdezett szakértők szerint habár a közigazgatási ajánlások számukra többnyire ismertek, de nem jelentettek kényszerítő erőt, körülményt, így költség és erőforrás hiányra hivatkozva gyakran pont a biztonsági megfontolások kerültek lehúzásra. Hiába indultak tehát be az elmúlt években a szakértők szerint egyértelműen pozitív folyamatok az elmúlt pár évben, ahhoz hogy ennek érezhető hatása legyen, még időre lesz szükség. A pozitívumok között említették a párbeszédet állam, a privát szektor és az oktatási/akadémiai szféra között, a preventív szemlélet és a tudatosítás fontosságának elismerése, valamint a holisztikus szemlélet, vagyis annak felismerése, hogy az

elektronikus információbiztonság szintjének emelése nemcsak a közigazgatásban, de a magánszektorban és az állampolgárok körében is ugyanolyan fontos.

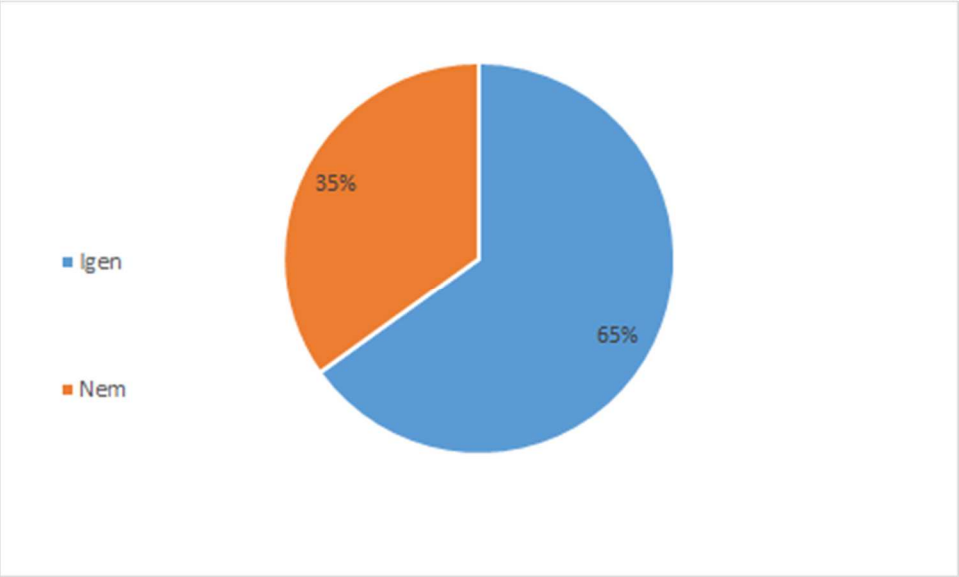
Például egy alkalmazott megoszthatja a hálózati jelszót, mert racionalizálja, hogy senki sem sérül meg, nem keletkezik káresemény a viselkedése miatt. Ezek az ésszerűsítések miatt a nem rosszindulatú alkalmazottak is tudatosan megsértik a biztonsági irányelveket. Viselkedésük ésszerűsítésével megpróbálják csökkenteni bűnösségüket vagy szégyenüket az informatikai politikák szándékos megsértése miatt. Ezen racionalizálások miatt viselkedésük normálisabbnak vagy szükségesebbnek tűnik, mint amilyen valójában (Siponen, 2010). Az egyértelmű dokumentumok és a következetesen betartott irányelvek, ellenőrzések és monitorozás mind olyan megközelítés, amely segíthet eltávolítani a kifogásokat az alkalmazottaktól, amelyek a nem megfelelő magatartás ésszerűsítése érdekében működnek.

Ezek összevágnak a saját megfigyeléseimmel, ahol az oktatások vagy biztonsági incidensek kivizsgálása során olyan indokok szoktak elhangozni:

- nekem nincs semmi fontos adatom amit védeni kellene,
- sehogy máshogy nem tudom elvégezni a saját feladatom, munkafolyamatom,
- más módon nem tudom időben végrehajtani a feladatom,
- az én adataim, hozzáférésem úgyse érdekel senkit, a hackereket se,
- ...

4.1.4 INFORMÁCIÓBIZTONSÁGI SZAKEMBER KÉRDŐÍV ELEMZÉSE

A 9. “Saját használatú / tulajdonú számítógépén van-e Önnek rendszergazdai joga?” kérdésre adott válaszok elemzése.



49. ábra: “Saját használatú / tulajdonú számítógépén van-e Önnek rendszergazdai joga?” kérdésre adott válaszok (%), forrás: saját szerkesztés

A 49. számú ábrán a válaszok százalékos eloszlása látható. Alapvetően nem javasolt a rendszergazdai jog megléte, így a 65% mindenképpen magas értéknek tekinthető.

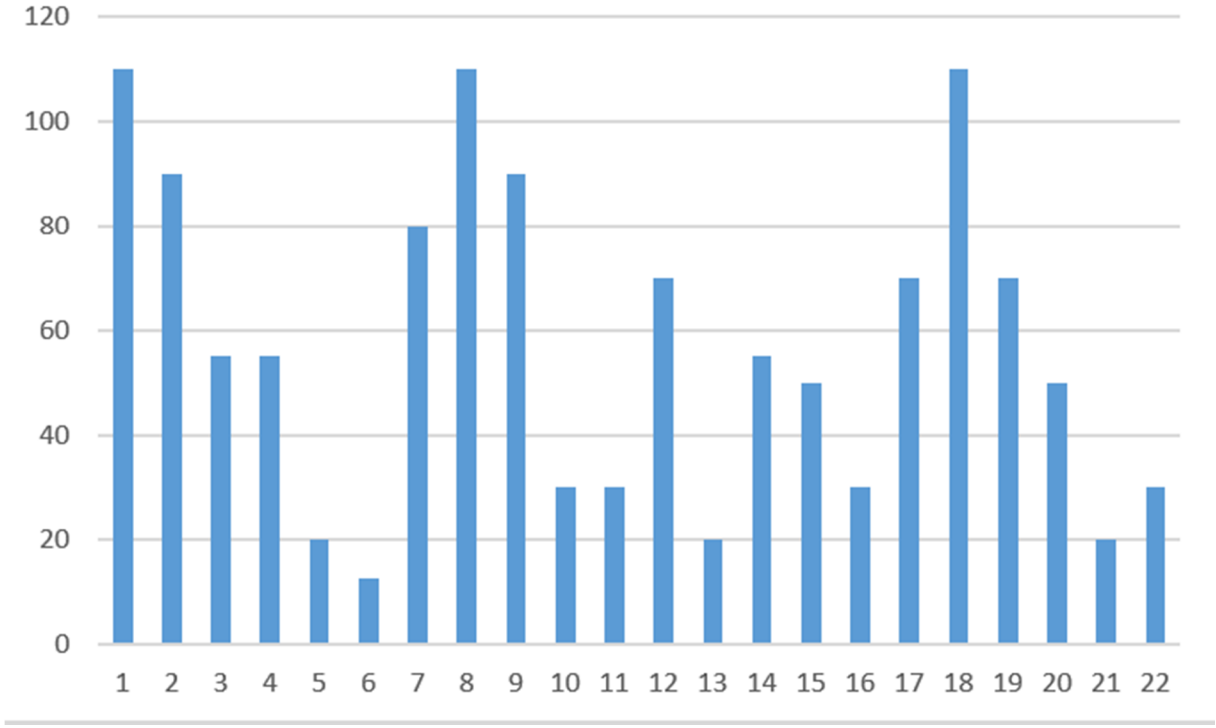
4.1.5. KÖZIGAZGATÁSI KÉPZÉS ELŐTT/UTÁN KÉRDŐÍV ELEMZÉSE

A kérdőív kapcsán két kérdésre adott választ kívánok kiemelni.

Az 1. "Hallott-e már régebben EU Safer Internet Programjáról?" kérdésre 6 fő válaszolta azt, hogy "Talán, már hallottam róla", míg 18 fő azt, hogy: nem. Az EU Safer Internet Program egy, az egész Európai Unióra kiterjedő kezdeményezés amely 2009 óta elérhető Magyarországon is. A válaszadók több, mint 60%-a a Ön miért döntött ezen oktatáson való részvétel mellett? kérdésre azt válaszolta, hogy gyermeke, családtagja miatt kíván részt venni a képzésen. Ennek ellenére egy az általános iskolák számára ingyenesen elérhető egész Magyarországra és az EU-ra kiterjedő programról nem is hallottak. Ugyanakkor a 10. "Tudta-e Ön, hogy a Safer Internet ingyenes képzéseket tart?" kérdésre, amely a tanulásra való hajlandóságot, a információbiztonsági tudásra való nyitottságot vizsgálta a válaszadók mindegyike azt választotta, hogy "Nem, de élnék a lehetőséggel".

Az információbiztonsági felkészültséget talán még jobban képes bemutatni, hogy mennyire tudnak a munkavállalók a rájuk vonatkozó szabályzatokról és munkáltatói elvárásokról. A 11. Ön szerint hány oldal terjedelmű az informatikai szabályzat? kérdésre, a 10 oldal és 150 oldal között lehetett választani 8 lehetőség közül. Helyes választ 3 választ mindössze 3 fő adott, (24 válaszadóból) mivel a szervezet akkor hatályos IBSZ-e 107 oldal terjedelmű volt.

A szervezetnél nem alkalmaztak (ezt megelőzően egyetlen egyszer sem) tantermi információbiztonsági oktatást, hanem a szabályzatot tették elérhetővé az intraneten. És az éves kötelező vizsga is az intranet oldalon volt elérhető. A vizsga fix kérdéseket tartalmazott, azaz a kérdések és helyes válaszok mindenkinél azonosak voltak a munkaszervezetben. Egyes vélemények szerint a megoldókulcs ismert volt a munkavállalók körében. Lemaradásként értékelem, hogy ha a közigazgatási szervezet munkavállalói nem ismerik, hogy milyen információbiztonsági szabályok és elvárások vonatkoznak rájuk, vagy hogy ezeket az elvárásokat honnan ismerhetik meg, hol tájékozódhatnak azokról.



50. ábra: "Ön szerint hány oldal terjedelmű az informatikai szabályzat?" kérdésre adott válaszok, forrás: saját szerkesztés

Az 50. számú ábrán a kapott válaszokat, a 24 válaszadóból 2 fő nem válaszolt, így 22 válasz eredményét, eloszlását ábrázoltam. A rendelkezésre álló mért és kvantifikált adatok, valamint a további rendelkezésre álló információk alapján, például, de nem kizárólag: a megoldókulcs közkézen forgása a munkaszervezetben, a sztenderd és fix vizsga kérdések és azok változatlan sorrendje, valamint az adott intranet aloldal, az információbiztonsági szabályzat látogatottsága, olvasottsága mint információ vezettek következtetésemig. Mindezek alapján arra lehet következtetni, hogy a munkavállalók az IBSZ hozzávetőleges nagyságát, oldalszámát, elérhetőségét sem ismerik. Valamint az oktatások és személyes megfigyelés során is azt tapasztaltam, hogy annak tartalmáról, elérhetőségéről sem rendelkeznek információval, az alkalmazott pusztán online elérhetővé tétele a szabályzatnak nem jutott el a munkavállalókhoz, vagy azt nem nyitották meg, annak helyét és tartalmát nem ismerték. Azaz nem önmagában csak az oldalszám ismeretének hiányában vontam le következtetésem. Ugyanakkor a szórás alapján elvárható lett volna, hogy valamilyen (a valós oldalszámhoz) konvergáló mintát kapjak. Ugyanakkor meg kell jegyezni, hogy az oldalszám, vagy annak nagyságrendi ismerete vagy hiánya önmagában nem alkalmas az információbiztonság szempontjából egyedüli és önálló indikátorként való felhasználásra.

Mindezek alapján HI hipotézisem nem sikerült alátámasztani, így azt elvetettem, hiszen statisztikailag bizonyított, hogy lemaradás tapasztalható sz információbiztonsági tudatosság

szintjének tekintetében a magyar közigazgatás területén a magyar üzleti szférával összehasonlítva a vizsgált mintában.

4.2. A MASODIK HIPOTÉZIS VIZSGÁLATA (H2)

„Every workplace has or should have information security policy, but without enough information security awareness, every policy is useless." Törley (2020)

Második hipotézisem (H2: A információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető, az írásbeli szabályozáshoz képest) bizonyítása során az eddigiekben alkalmazott logikát sorrendet alkalmazom. Ennek során végigveszem azokat a releváns kutatásokat, melyeket elvégeztem valamint azon kutatásokat amelyekben részt vettem és figyelembe veszem a szakirodalmi áttekintés során megismert eredményeket is, azokat megfelelő mértékben meghivatkozom.
A bizonyítás jobb megértéséhez és a gondolati ív pontos dokumentáltsága miatt így kitérek több kisebb fogalomra, jelenségre, amelyek relevánsak.

Az egyes kutatások releváns részeinek bemutatása előtt fontosnak tartom - nagyon röviden - bemutatni, az általam tapasztalt gyakorlatot. Megfigyeléseim alapján ez az általánosan elterjedt gyakorlat vagy tipizálható hibák az írásbeli szabályzatok kiadása kapcsán.

- új szabályzatként jelenik meg az információbiztonsági szabályzat, előtte külön szabályzata nem volt,
    - (létezett szokásjog vagy írásbeli szabályozás,)
- elkészítése (frissítése) csak a legszűkebb környezet bevonásával történik meg, jog, informatika,
- kiadása a szervezet kiadási, köröztetési eljárásának megfelelő, de így csak a felsővezetők kapnak róla értesítést, esetleg megjelenik az intraneten, ill. a szabályzat tárban,
- a végfelhasználók tömegei és középvezetők nem kapnak róla tájékoztatást, a középvezetők esetleg továbbított üzenetként kapják meg a területi felső vezetőtől,
- az adott szerepkörben releváns információbiztonsági taratlom, vagy annak alkalmazhatósági vetülete nincs ismertetve széles körben, szabályalkalmazási gyakorlat (tréning) nincs,
- az információbiztonsági szabályzatnak kivonata nem áll rendelkezésre.
- a szabályzat türelmi, bevezetési időt nem tartalmaz,
- a szabályzat a belső audit, bevezetési, alkalmazási elvárásokat nem tartalmazza, vagy nincs összhangban.

Tehát a tipizálható jegyek egy átlagos kkv-t elérő létszámú munkaszervezet esetén:

- információbiztonsági szabályzat létrehozása vagy frissítése utána a vállalat intranet oldalán elérhetővé válik,
- felső, vagy középvezetői kör kap róla jellemzően e-mailes tájékoztatást,
- az éves információbiztonsági képzés során gyakran csak írásban kapnak tájékoztatást, oktatást a munkavállalók.
- az információbiztonsági szabályzatnak kivonata nem áll rendelkezésre.

Mindezeket egyrészt információbiztonsági szakértői munkám során több tucat szervezetben tapasztaltam, azonban ezen kívül két Magyarországi vállalatnál "A" company és "B" company esetében lehetőségem volt kutatás keretében megfigyelni az információbiztonsági szabályzat és információbiztonsági politika kiadási folyamatát, annak során keletkező megfigyeléseket kvantifikálni. Ezeket tudományos alapossággal összevetettem azon számadatokkal amelyek a tantermi oktatás során keletkeztek.

Így tehát vizsgáltam olyan szervezetet,

- ahol az információbiztonsági szabályzat kiadásra került, ott előtte és utána idősoros vizsgálatot bemutatom,
- ahol e-learning oktatás került publikálásra, ott előtte és utána idősoros vizsgálatot bemutatom,
- ahol élő oktatás került megszervezésre, ott előtte és utána idősoros vizsgálatot bemutatom.

Így tézisemben azt vizsgálom, hogy az szervezet esetében ahol csak írott szabályzat került publikálásra míg a másik szervezetben élő oktatás keretében került megvalósításra, hogyan változott a szabályalkalmazás gyakorlata.

Így az "A" vállalatnál időben elkülöníthető szakaszok:

- nem volt információbiztonsági szabályzat (1. intervallum)
- kidolgozásra, majd kiadásra került információbiztonsági szabályzat (a szervezet intranet oldalán) (2. intervallum)
- tantermi képzés került lebonyolításra, (3. intervallum)
- tantermi képzés közben és után mért adatok kiértékelése (4. intervallum)

Így az "B" vállalatnál időben elkülöníthető szakaszok:

- nem volt információbiztonsági szabályzat (1. intervallum)
- kidolgozásra, majd kiadásra került információbiztonsági szabályzat (a szervezet intranet oldalán) (2. intervallum)
- 1. e-learning képzés kiadásra került, (3. intervallum)
- 2. e-learning képzés kiadásra került, (4. intervallum)
- az e-learning közben és után mért adatok kiértékelése (4. intervallum)

51. ábra:Vizsgált időintervallum--szakaszok, "A" és "B" vállalat esetében, forrás saját szerkesztés

Az 51. számú ábrán összefoglalom a szabályzat nélküli, a szabályzat kiadását és a képzési időszakot jellemző időbeli intervallumokat.

4.2.1. ON-LINE KÉRDŐÍV ELEMZÉSE

Ahogy disszertációmban bemutattam a jelszókezelés jó indikátora az információbiztonsági tudatosságnak, szabályalkalmazásnak. Ennek megfelelően vizsgáltam kutatásom során a jelszókezeléssel kapcsolatos gyakorlatot a már bemutatott online kérdőívem segítségével. Valamint a hazai és nemzetközi szakirodalomat áttekintve hasonló eredményeket találtam Szász és Kiss (2018) jelszóval kapcsolatos szabályalkalmazási gyakorlati megfigyelései kapcsán is.

Bemutatom a H2 tézis kapcsán releváns kérdéseket.

A 2.33 Honnan származnak a jelszóval kapcsolatos ismereteid?

A 2.35 Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? kérdésre adott a közigazgatáson belül kapott válaszokat tovább, hogy milyen számosságot és mintát mutat azok köre, akik bár kaptak képzést, (152 fő), de nem jelölte meg azt, mint ismeretforrás, ez 32 válaszadó volt, amely a teljes minta szempontjából igen magasnak tekinthető. Ugyanezen kérdést vizsgáltam az Ismerőstől, baráttól, mint információforrástól származó ismeretek tükrében is, ahol 30 válaszadó mondta, hogy kapott képzést, de jelszóval kapcsolatos ismeretei (részben) ismerőstől, baráttól származnak.

Azon csoporton belül, akik kaptak képzést és megjelölték, hogy jelszókezeléssel kapcsolatos ismereteik jelszóval kapcsolatos ismereteik származási helye: képzés, 120 fő, több mint fele 64 fő valamely egyéb forrást is megjelölte ezen ismeretek forrásaként.

Ez összhangban van azon állításommal, hogy a csoportnorma jelentős hatással van az egyén információbiztonsági szabályalkalmazási gyakorlatára. Fontos, hogy szándékosan alkalmazom a "szabályalkalmazási gyakorlat" kifejezést és nem a tudatosságot, mivel, mint látni fogjuk ezen tézisemnél pontos ez a különbség lesz még jobban kimutatható, mintha pusztán a tudatosságot (szabály ismeretet) vizsgálnám.

Az is látható további kérdésekből, hogy a 384 főből 120 fő kapott képzést, és a teljes mintán látható, hogy nagyon komoly, erős elvárásaik vannak a saját jelszavaikkal kapcsolatosan, "A jelszavamtól elvárom, hogy ...

2.4 ... legyen biztonságos.

2.5 ... legyen megjegyezhető.

2.6 ... feleljen meg a jó jelszó elvárásainak.

2.7 ... meg tudjam védeni az adataimat."

valamint a 2.24-2.32 kérdések figyelembevételével és bemutatásából ez a következtetés levonható. Azonban az információbiztonsági tudatosság indikátorára, a jelszó "jóságára" minőségére vonatkozó kérdésekre már rendkívül gyenge válaszokat tudtak csak adni. Tehát vagy az oktatáson nem kaptak erre vonatkozó megfelelő instrukciókat, vagyis csak formális oktatás lehetett, de a gyakorlatban azok az ismérvek ismeretek nem kerültek átültetésre, nem váltak a napi gyakorlat részévé.

Kutási kérdésemmel tehát pontosan ezt kívánom megvilágítani, hogy vagy a hiányzó szabályozás, vagy a meglévő szabályozás, vagy a hiányzó oktatás, vagy a megtartott, de nem megfelelően megtervezett oktatás, (tréning, alkalmazási gyakorlat hiánya) amikor a bevonódás elmarad. Vagy a kipróbálás, alkalmazási gyakorlatba való átültetés elmaradt. Vagy a gyakorlatba (saját munkafolyamataiba) nem képes a munkavállaló a kapott információt átültetni, az ilyen gyakorlati hiányosság rendkívül rossz eredményeket hozhat, amelynek magas az információbiztonsági kockázata. Kutatásaim és saját tapasztalatom is alátámasztja, ahogy a szakirodalom is, hogy ha olyan oktatáson van lehetősége részt venni a munkavállalónak, ahol a bevonódás megtörténhet, akkor a gyakorlatba épülés, a kötődés erősebb lesz, (Szász, Kiss 2018). Ezt a későbbiekben a kidolgozott modellem alkalmazását követő számszerűsíthető értékekkel bemutatásával is bizonyítom.

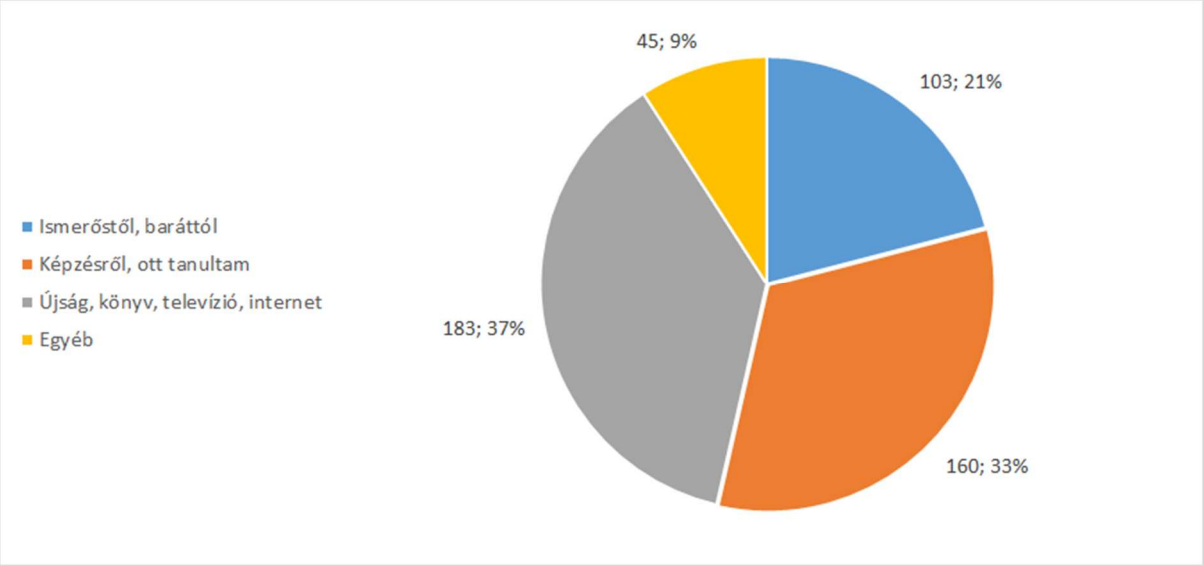
2.33 "Honnan származnak a jelszóval kapcsolatos ismereteid?" (Több válasz is lehetséges!) A kérdésre az alábbi válaszokat kaptam (közigazgatási szférán belül):

Ismerőstől, baráttól: 103

Képzésről, ott tanultam: 160

Újság, könyv, televízió, internet: 183

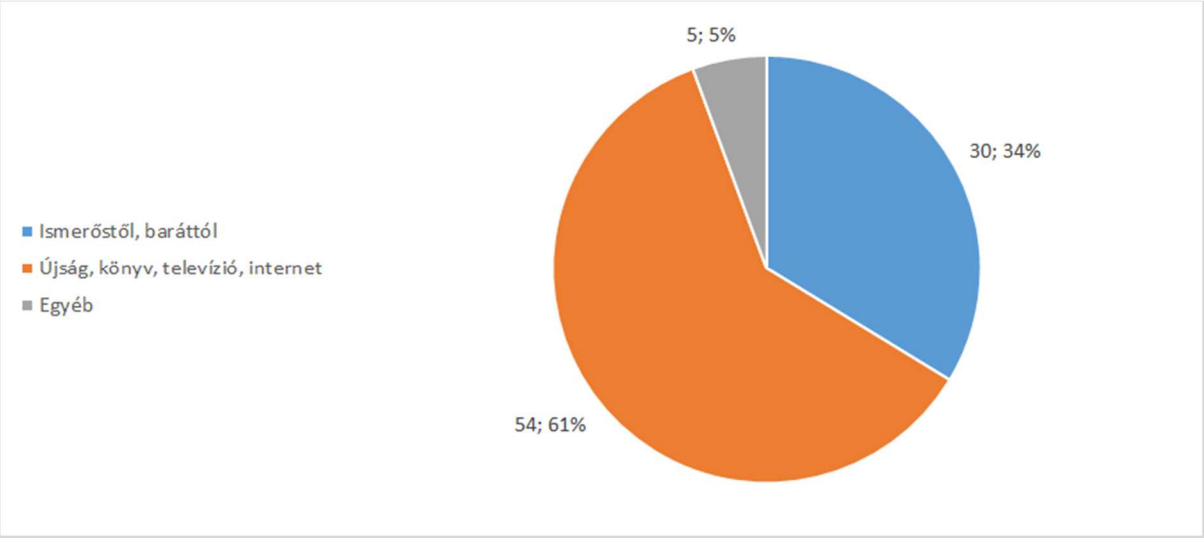
Egyéb: 45.



52. ábra: "Honnan származnak a jelszóval kapcsolatos ismereteid?" kérdésre adott válaszok (%), forrás: saját szerkesztés

Az 52. számú ábrán a jelszóval kapcsolatos ismeretek forrásának százalékos megoszlását mutatom be a közigazgatásban dolgozó válaszadók alapján.

Ha azonban a csoporton belül szűkítést alkalmazok és azokat vizsgálom, akik Ismerőstől, baráttól (is) szereznek jelszóval kapcsolatos ismereteket, akkor az egyébként nem a matematikailag indokolhatónak tűnő közel felezős vagy harmadolós arányszámot kaptam:



53. ábra: "Honnan származnak a jelszóval kapcsolatos ismereteik azoknak, akik nem kaptak képzést? (%), forrás: saját szerkesztés

Az 53. számú ábrán azon válaszadókat darabszám és százalékos eloszlását mutatom be, akik nem kaptak képzést.

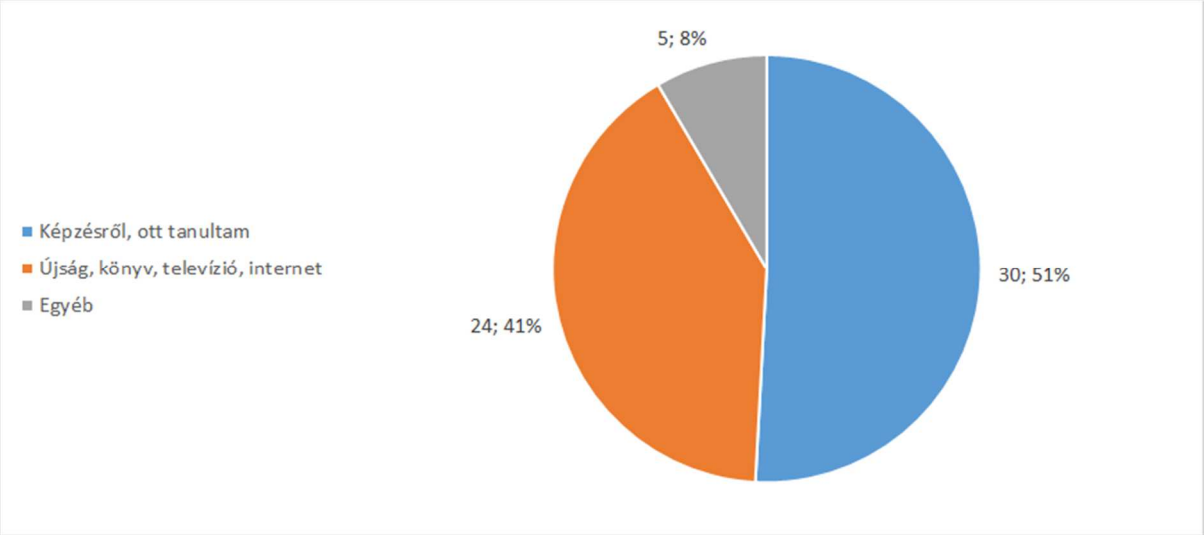
Ismerőstől, baráttól: 30 (103)

Újság, könyv, televízió, internet: 54 (183)

Egyéb: 5 (45)

Zárójelben az eredeti értékeket tüntettem fel, hogy még jobban látható legyen a nagyságrendi változás.

Ezek után elvégeztem ellenkező irányban is a csoport szűkítését és a vizsgálatot. Tehát azokra szűkítettem a vizsgálatot akik saját nyilatkozatuk szerint képzésről szerezték ezen ismereteiket.



54. ábra: "Honnan származnak a jelszóval kapcsolatos ismereteik azoknak, akik kaptak képzést?" (%), forrás: saját szerkesztés

Képzésről, ott tanultam: 30 (160)

Újság, könyv, televízió, internet: 24 (183)

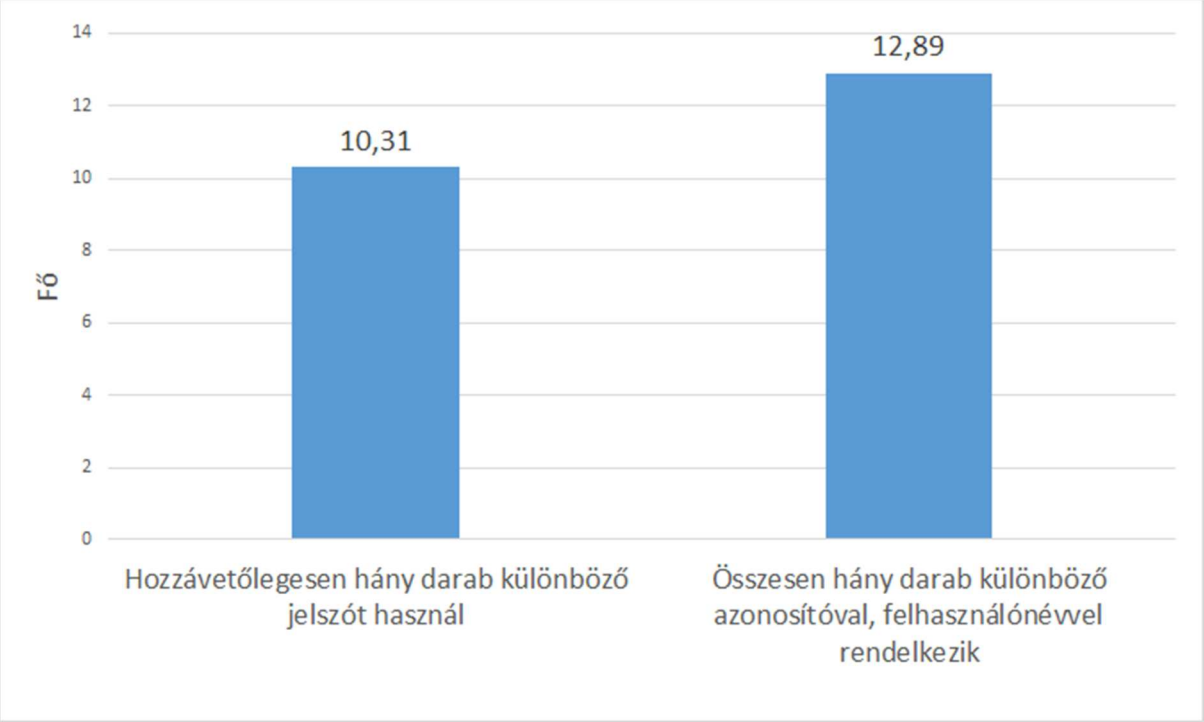
Egyéb: 5(45)

Ezt követően úgy döntöttem, hogy már fókuszáltan szükséges úgy vizsgálni a válaszadókat, hogy akik kaptak-e oktatást és akik nem kaptak oktatást az egyes információbiztonsági kulcsterületeken, azaz a jelszó létrehozással, kezeléssel, tárolással kapcsolatos attitűdjük mennyiben mutat eltérést.

Megvizsgálva azokat akik kaptak oktatást, (152 fő), csak 59 fő (39%) mondja azt, a 2.14-es kérdésben, hogy "Hallottál-e már jelszószéfről (jelszókezelő programokról)?" és ebből csak 17 (29%) fő válaszolt igennel arra a kérdésre, hogy 2.15 "Ha hallottál a jelszószéfről, akkor használod-e?" mondja, hogy használja is azt. Ismét az derült ki, hogy a kapott oktatás nem terjedt ki alapvető fontosságú területre, vagy nem volt eléggé gyakorlat orientált, hogyan lehetséges a jelszavakat megfelelően kezelni.

Megvizsgálva azokat, akik kaptak oktatást, (152 fő), (ebből 59 fő hallott, de csak 17 fő használ jelszó kezelésre alkalmas programot). Megítélésem szerint ez az egyre csökkenő tendencia egyrészt az oktatás és támogatás hatásfokára, másrészt a szokás (eszközhasználat) kialakulásának nehézségeire vezethető vissza, amely bár kutatásomnak nem volt tárgya, azonban későbbi, további kutatások tárgya lehet.

A felhasználónkénti jelszó darabszám és felhasználónkénti azonosító darabszám kapcsán az átlagos jelszó szám / felhasználó : 10,31 (2.1 Hozzávetőlegesen hány darab különböző jelszót használsz?) míg a (2.37 Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)) kérdésre adott 12,89.



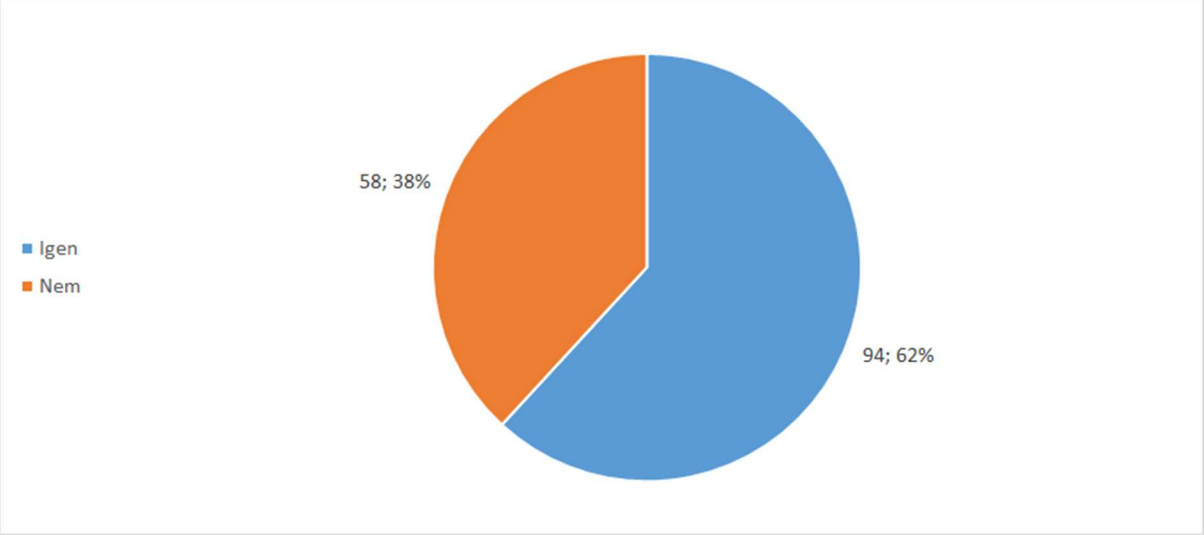
55. ábra: Két kérdés vizsgálata az oktatást kapottak között, forrás: saját szerkesztés

Az 55. számú ábrán az azonosítók és jelszavak számának aránya olvasható le, az oktatást kapottak közül. Ez azt is jelenti, hogy bár kaptak oktatást, 1882 darab rendszerhez csak 1568 jelszót használnak és azt sem megfelelő módon kezelve. A kérdésfeltevés során további szempont volt, hogy külön, időben és térben távolabb kerüljenek bizonyos, ugyanazon tudásblokkot feszegető (kontroll) kérdések, ahogy a 2.1 és 2.37-es kérdés is mutatja.

Ezek mind azt mutatják meg, hogy a kapott oktatás nem a megértésre a szabályalkalmazás gyakorlatára fókuszál vagy nem nyújt elegendő támogatást ahhoz,hogy azt az egyén elkezdje alkalmazni, vagy nem azonosul, nem ért egyet a szabállyal, nem látja értelmét az alkalmazásának.

Tovább vizsgálva a képzést kapottak csoportjákt és jellemző viselkedési motívumaikat a jelszóhasználati szokásokon, mint indikátoron keresztül vizsgálva, Megvizsgálva azokat akik kaptak oktatást, (152 fő), 94 fő válaszolt igennel arra a kérdésre, hogy 2.42 “Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?”, amely egyértelműen nagyon komoly problémát jelent, és egyértelműsíti a jelszóhasználat, mint indikátor használatán túl azt is, hogy rendszerszintű a probléma. 62%-a már volt, hogy megadta a jelszavát,

amely egészen elképesztően magas érték. Hiszen alapvető elvárás, hogy az azonosító amely emberhez van rendelve az azért elkövetett, végrehajtott cselekményekért az azt átvevő személy tartozik felelősséggel.



56. ábra:"Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?" kérdésre adott válaszok az oktatást kapottak körében, forrás: saját szerkesztés

A 56. számú ábrán a jelszómegosztást reprezentáló ábra. Tekintve, hogy alapvetően tiltott a jelszó, azonosító megosztás bármely megnyilvánulása, így mindenképpen komoly gond, hogy a képzésben résztvevőknél is rendkívül magas.

A 2.8 "Hány karakter a legrövidebb jelszavad?" kérdésre ugyenezen csoporton vizsgálva azokat akik kaptak oktatást, (152 fő), 7,05 karakter az átlagos jelszó hosszúság a legrövidebb jelszóra. A közigazgatásra szűkített teljes 384 fő ez a szám 7,23, azaz nem mutat szignifikáns emelkedést az, hogy kapott-e oktatást. Ugyenezen számadatok a 2.9 "Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?" esetében pedig 10,12 és 10,14-es értéket mutat, még tovább csökkentve a különbséget. Mindez továbbra is a azt támasztja alá, hogy a jelenléti, mélyebb bevonódás hatékonyabb.

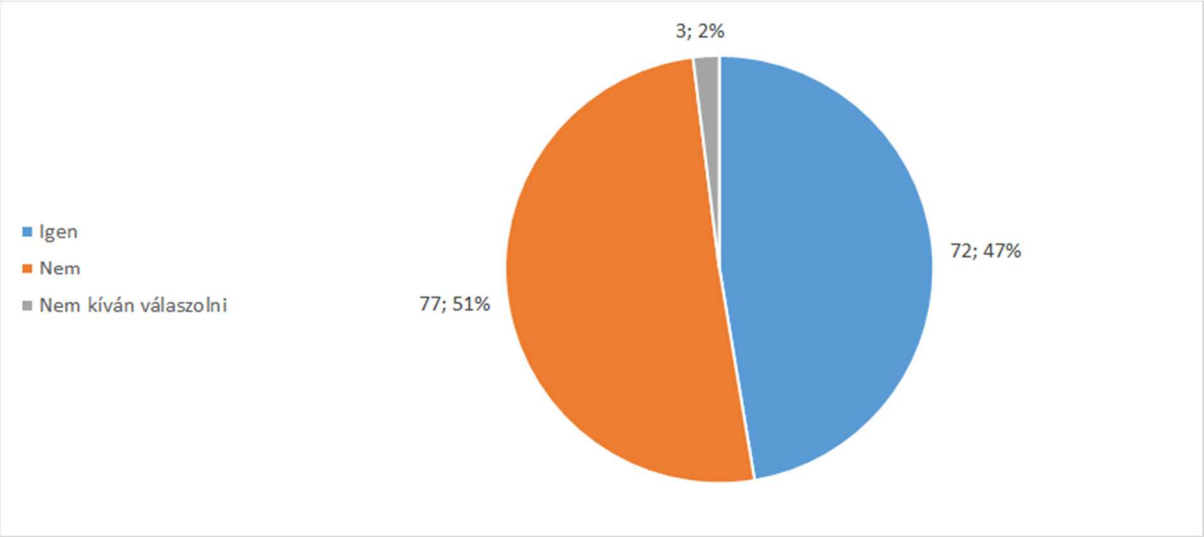
Szász-Kiss (2018) kutatásában kimutatta, hogy 68,4%-a a csoportnak hosszabb jelszavakat kezdett használni, ha a képzésbe való bevonódás lehetősége adott volt a képzésen, míg a kontroll csoportban a résztvevők 63,0%-nál nem volt változás.

A 2.10 "Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?" kérdésre Megvizsgálva azokat akik kaptak oktatást, (152 fő),a közigazgatási csoporton belül 107 fő (70%) válaszolt igennel, 36 fő (24%) válaszolt nemet és 9 (6%) fő nem kívánt válaszolni.

Ha ezt a teljes válaszadói mintán nézzük, 275 fő (62%) válaszolt igennel egy olyan 445 fős csoportból akik kaptak oktatást. Amiből az is látszódik, hogy a közigazgatásban tapasztalható gyakorlat rosszabb, mintha a teljes mintán nézzük.

Megfigyeléseim alapján a jelenléti oktatás során csoportmunkában, amely a bevonódást elősegíti a csoport aktívan és kooperatívan képes összeszedni a jelszóra (annak létrehozására, kezelésére, tárolására, stb.) vonatkozó ajánlásokat. Akár 5-15 állítást jellemzően. Azonban ennek gyakorlatba ültetése, hogy az adott ajánlást hogyan lehetne megvalósítani az már nem megy. Véleményem szerint ennek az az oka, hogy míg a szabályzat olvasáskor, annak ismertetésekor, visszajátszott videós előadáskor, vagy bármilyen olyan módszernél ahol nem lehetséges a kérdésfeltevés, vagy aktivizálódás, bevonódás ott az elmondot szabályok még akár szövegszerű állítósokként megmaradnak és emlékezhetnek rá bizonyos esetekben, de a gyakorlatba kevésbé tudnak beépülni. Továbbá szintén oktatásokon történő megfigyelésem, ha az adott szabállyal kapcsolatban lehetőség van megmutatnia, hogy miért is szükséges, pl.: mert az 6 karakteres jelszó visszafejtési ideje 3 perc (az általam szimulált környezetben), akkor a nem pusztán szabályközlés, hanem a miértre való bemutatás miatt jobban rögzül, bevonódással pedig igyekszik a bemutatott kockázatot elkerülni. Azaz a szabály mögötti kockázatot is megérti, valósnak kezdi el érzékelni, úgymond nem csak üres szabály marad.

A 2.19 “Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?” kérdés a közös használatú jelszavakra vonatkozott. Amely ugye egyértelműen szabályellenes, mivel a személyre kiadott hitelesítési eszközzel járó felelősséget nem lehet megosztani. 72 fő válaszolt igennel, 77 fő nemmel és 3 fő nem válaszolt.



57. ábra: „Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?” kérdésre adott válaszok, forrás: saját szerkesztés

Az 57. számú ábráról leolvasható, hogy 47%-a a felhasználóknak ezt a legalapvetőbb ajánlást nem tartja be a kapott oktatás ellenére. Ennek számos oka lehet, hogy a disszertációmban kifejtem a szabályzat helytelen kialakítása, a munkafolyamatok felmérésének hiánya, annak nem megfelelő kommunikáció, a szabályzat elérhetetlensége. Ilyen esetekben a szabályzatszegés, a racionalizás révén fel sem tűnik, hogy milyen komoly gond van, mint például jelen esetben ki lett mutatva.

Disszertációmban voltaképpen azokat a mély miértekre és gyökérokokra próbálok rávilágítani amelynek megértése és feltárása alapja lehet egy olyan transzfomációhoz amelyre szükség van a szokások és mélyben megbúvó. alattomos rossz gyakorlatok, csoportnormák megváltoztatása érdekében.

A 2.24 “Ha megbízható emberekkel használok közös jelszót, az nem jelent biztonsági kockázatot.” kérdésre a közigazgatáson belül oktatást kapott emberek közül választ adokkat átlaga 2,21, azaz egyértelműen a “nem értek egyet” részhet tart. Ugyanakkor az intervallum jobb felére 38 fő adott választ. Ugyanezen értékeket a teljes közigazgatási mintán belül a nem oktatást kapottakon vizsgálva 57 fő.

Kiemelném, hogy a “Teljes mértékben egyetértek”, az intervallum jobb végére összesen az oktatást kapottak közül 4-en, egyébkétn pedig a teljes köz9g mintából 20-an választották.

Ebből következik és alátámasztott, az oktatás szükségessége, jól mutatják a nagyságrendek, a nem oktatottak körében 4-szeres a “rossz választ” adók száma. Ugyanakkor az általánosan elterjed gyakorlat a teljes közig mintán is tömegeket érinthet. Azaz egyrészt tetten érhető a lemaradás és a felzárkóztatás szükségessége. És ezzel együtt az is számszerűsíthető, hogy nem elegendő a szabályok ismerete, hanem annak ‘megértése’ a szükségesség alátámasztása, az alkalmazhatóság érdekében annak támogatása, hogyan tudja a saját munkafolyamataiban az adott munkavállaló (akár munkakörönként eltérő módon) felhasználni, alkalmazni.

A 2.25 “Minden helyre különböző jelszót használok.” kérdésre 124-en válaszoltak a közig mintában oktatást kapottak közül, ennek átlaga 3,89, közel median. Amely azt igazolja, hogy bár a szabályokkal, elvárásokkal nagyságrendileg tisztában vannak, hogy minden különböző információs rendszerhez különböző jelszót kellene használni, a gyakorlat ahogy előzőekbe be lett mutatva nagymértékben eltér az elmélettől, de közelebb van a “Teljes mértékben egyetértek” állításhoz a 0-6 zárt intervallum tekintetében. Az oktatást nem kapottak esetében az előbbi számok 175 válaszadásra és 3,42-es átlagra módosulnak. Amennyiben pedig nem csak a közig mintán vizsgálom az oktatást kapottak száma akkor 370 a válaszadók száma, az átlag pedig az átlagos támogató elfogadás 3.8-ra emelkedik. Az oktatás hatása itt is pozitívan befolyásolja a tudatosságot.

2.28 Saját belátásod szerint, mennyire vagy tisztában a jó jelszóval kapcsolatos elvárásokkal? kérdésre adott válaszokat (a teljes mintán) vizsgálva az oktatást kapottakon belül az átlaga 5,23 a válaszadók közül.

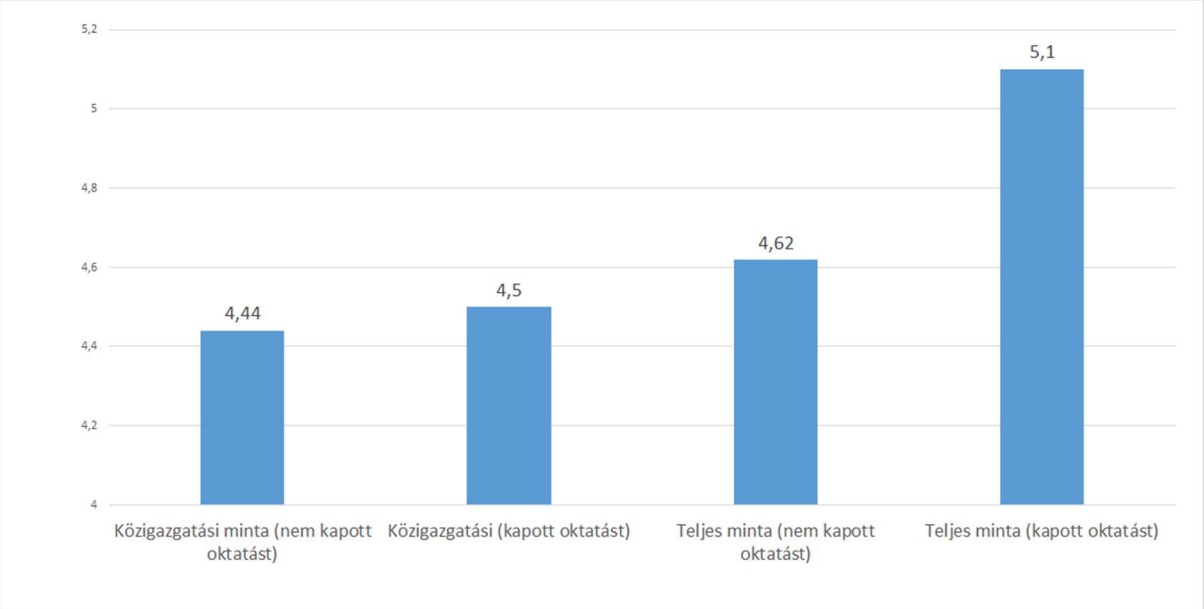
Azok közül akik nem kaptak oktatást ez az érték alacsonyabb 4,90.

A közigazgatási mintán megismételve az előbbi két érték az oktatást kapottak esetében 5,0, azaz alacsonyabb, mint a teljes mintán vizsgálva. Azok közül akik nem kaptak oktatást ez az érték alacsonyabb 4,75. Azaz a közigazgatásban mind az oktatást kapott, mind az oktatást nem kapottak úgy nyilatkoztak, hogy kevésbé vannak tisztában a jó jelszóval, jelszókezeléssel kapcsolatos elvárásokkal.

Ugyanakkor az is látható, hogy az oktatás révén tisztába kerülhetnek az elvárásokkal, ez egyértelműen látszódik is, hogy tisztában vannak, (azt gondolják) de az előbbi kérdések kiértékelése során az is bizonyítást nyert, hogy a gyakorlatba már nem, vagy nehézkesen tudják az így megszerzett ismereteket átültetni.

2.29 Nagyon jók és biztonságosak a jelszavaim kérdésre az oktatást kapott és nem kapott felhasználók között nincs nagyságrendi különbség. 4,74 és 4,78-ak az értékek. Tehát míg a 2.28 Saját belátásod szerint, mennyire vagy tisztában a jó jelszóval kapcsolatos elvárásokkal? kérdésre az oktatást kapott és nem kapott felhasználók között 4,58 és 5,0 átlagos értéket adtak. Ezen eltérések jól mutatják, hogy bár az oktatást kapottak úgy gondolják, hogy jobban tistában vannak az elvárásokkal, de a gyakorlatban való alkalmazásra rákérdezve, hogy valóban mennyire tartja biztonságosnak a jelszavait elenyésző 0,04 a két minta különbsége. Ez jól mutatja, hogy a gyakorlatba, szokásba való átültetés, a munkafolyamathoz való illesztés már egy, a hagyományos frontális és egyirányú oktatástól elkülönülő tevékenység kell, hogy legyen.

2.30 Az érzékenyebb, fontosabb adatokhoz hosszabb jelszót szoktam használni. kérdésre



58. ábra: Az érzékenyebb, fontosabb adatokhoz hosszabb jelszót szoktam használni." pontra, adott válaszok (likert skála adat), forrás: saját szerkesztés

közig minta, az oktatást kapottak: 4,5

közig minta, oktatást nem kapottak: 4,44

teljes mintán az oktatást kapottak: 5,10

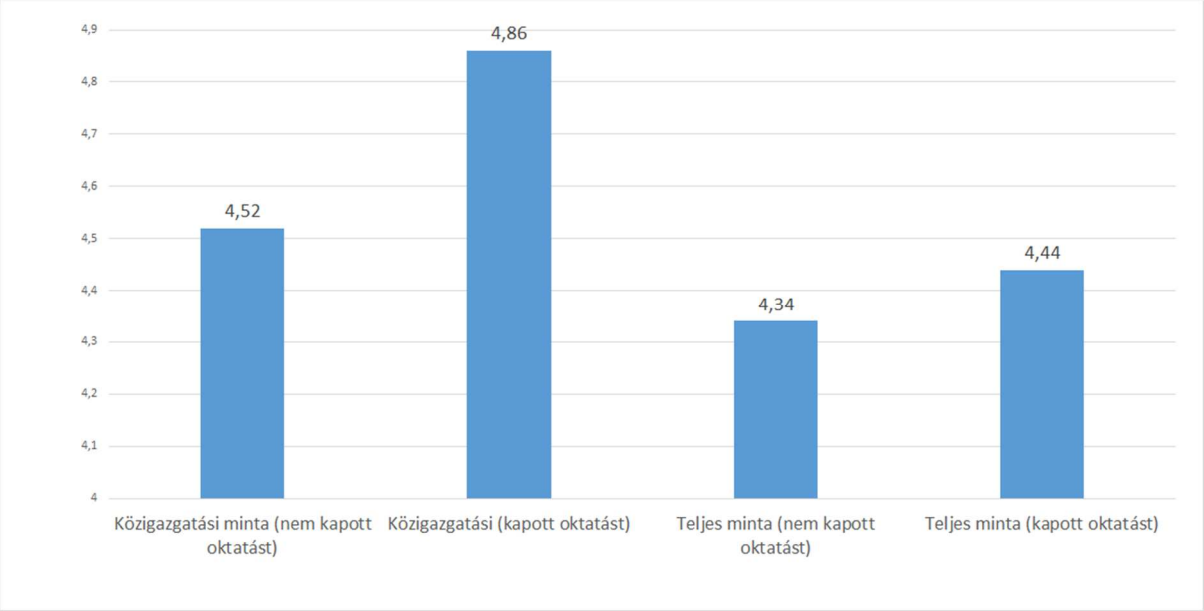
teljes mintán oktatást nem kapottak: 4,62

A 2.12 Használsz-e valamilyen jelszóképzési szabályt annak érdekében, hogy ... ... könnyen megjegyezhető legyen a jelszavadat? és 2.13 ... biztonságos legyen a jelszavad? kérdéseknél pontosan ezt kívántam vizsgálni, hogy a gyakorlatban mennyire alkalmazható tudássá képes az egyén átforgatni. A kérdőívre adott válaszokból látható, hogy kis százalékban használnak valamilyen jelszókezelésre alkalmas eszközt, jelszó széfet. Így a jelszavakat valamilyen más módon 'jegyzik meg'. Vagy valamilyen egyéb stratégia szükséges, hogy a minden rendszerhez különböző jelszó ajánlás tartható legyen. 13,06 különböző rendszer használnak a közigazgatási válaszadók átlagosan. Ha ehhez még megvizsgáljuk a 2.18 Milyen sűrűn változtatod meg (általában) a jelszavaidat? kérdést, ahol a naponta (1), hetente(2), havonta (3), Negyed évente (4), évente (5), Ritkábban, mint évente (6), Soha (7), nem mondom meg (8) értéket vehette fel. 12 fő nem kívánt válaszolni (8), az átlagszámításból így a 8-as érték kizárásra került. Ez kiszámítva az átlagos érték 4,56. Tehát a negyed évente és évente között, az évenkénti változtatáshoz közelebb. Ugyanakkor 61 válaszadó adott 5-7 intervallumból vett értéket. Azaz 40% nem tartja be, nem alkalmazza a jelszóváltoztatásra vonatkozó ajánlást a kapott oktatás ellenére.

A jelszó velünk együtt öregszik. Az „adatlopás", mint az adatokhoz való hozzáférés egy paradox kifejezés, hiszen a legtöbb esetben az adatokat nem lopják el a klasszikus értelemben,

hanem megmaradnak; azonban illeték is hozzáfér azokhoz. Minél hosszabb egy jelszó élettartama, annál jobban megnő a „közös” illetéktelen használat veszélye, visszafejtés, hash megszerzése által, vagy egyéb módon.

2.31 Figyelembe veszed-e új jelszó megadásánál, ha mutatja az adott alkalmazás a jelszó erősségét?



59. ábra: Figyelembe veszed-e új jelszó megadásánál, ha mutatja az adott alkalmazás a jelszó erősségét? kérdésre adott válaszok, forrás: saját szerkesztés

közig minta, az oktatást kapottak: 4,86

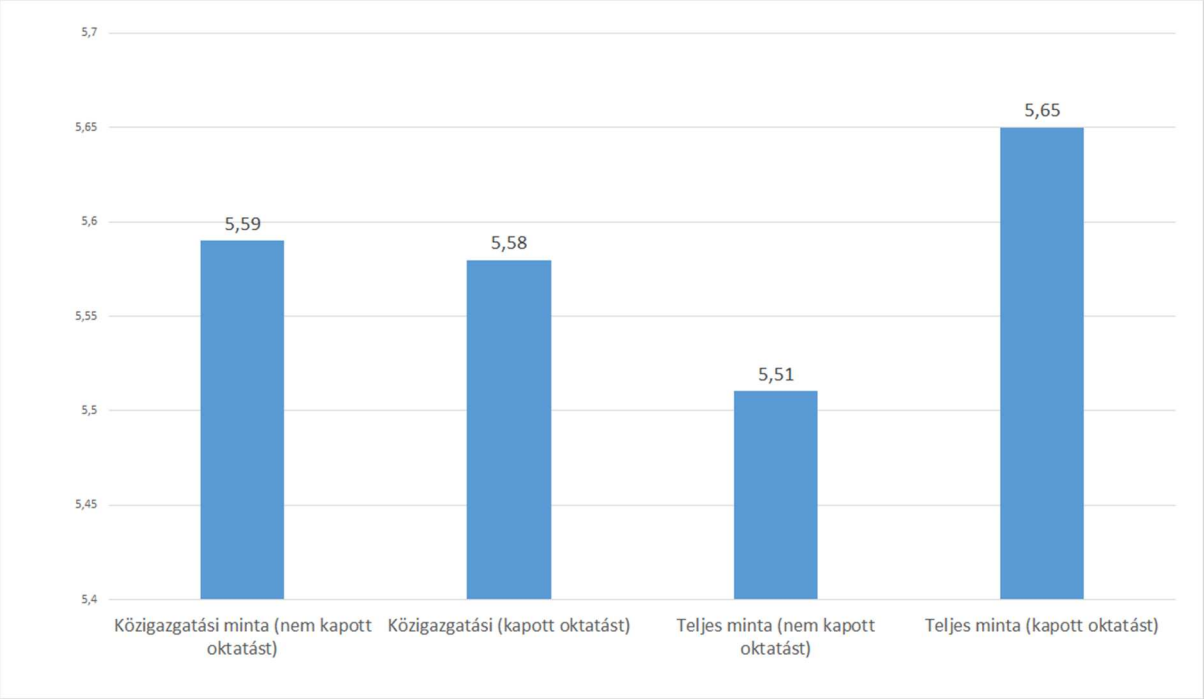
közig minta, oktatást nem kapottak: 4,52

teljes mintán az oktatást kapottak: 4,44

teljes mintán oktatást nem kapottak: 4,34

Itt is igazolódni látszik, hogy az oktatáson kapottakat elméletben tudják, “figyelembe veszik”, de az alkalmazási képességét láthattuk a fentiekben már, hogy elmarad.

2.32 Mennyire jellemző, hogy törekszel az erős jelszóra?



60. ábra: "Mennyire jellemző, hogy törekszel az erős jelszóra?" kérdésre adott válaszok, forrás: saját szerkesztés

közig minta, az oktatást kapottak: 5,58

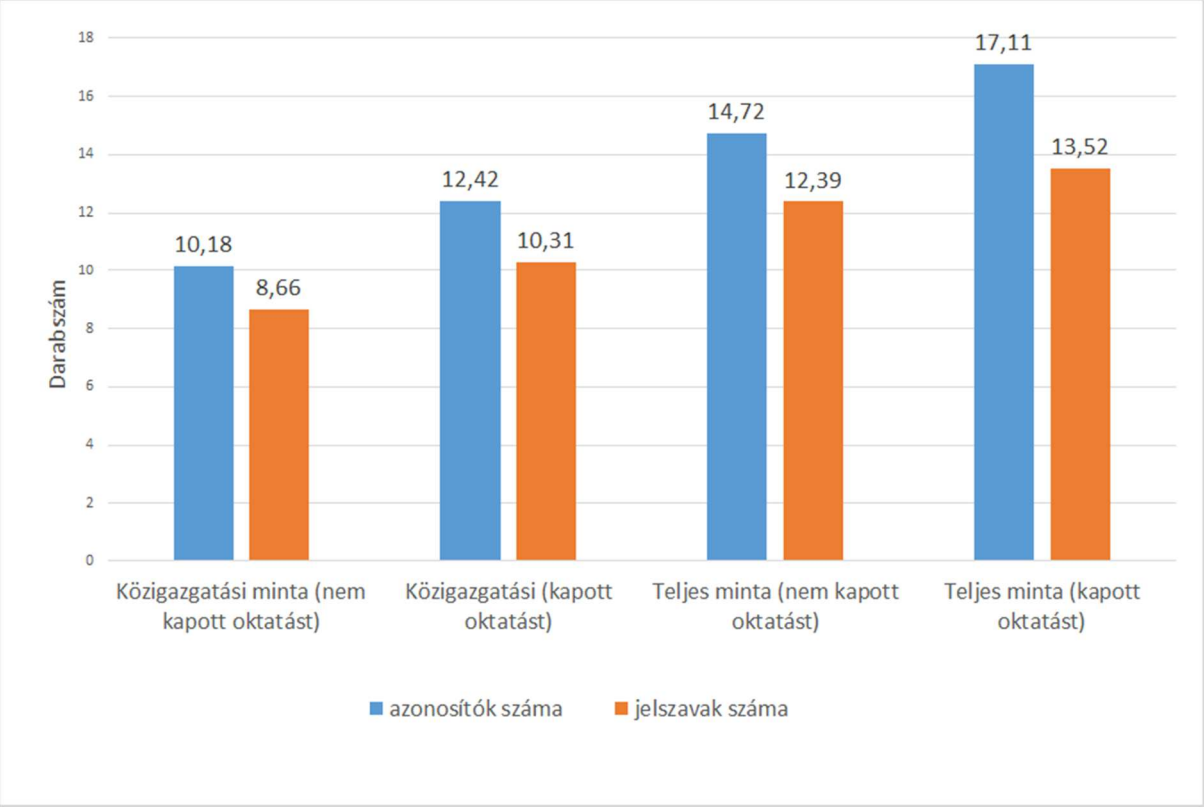
közig minta, oktatást nem kapottak: 5,59

teljes mintán az oktatást kapottak: 5,65

teljes mintán oktatást nem kapottak: 5,51

Ez is beleillik a logikai sorba, hogy törekszik, megvan a belső indíttatás, a szándék, de nem tudja, hogyan lehetséges ezt a gyakorlatban alkalmazni.

A 2.37 Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.) kérdést a 2.1 Hozzávetőlegesen hány darab különböző jelszót használsz? kérdés tükrében vizsgálom.



61. ábra: Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? valamint a Hozzávetőlegesen hány darab különböző jelszót használsz? kérdésre adott válaszok a teljes mintán ill. a közigazgatásban, forrás: saját szerkesztés,

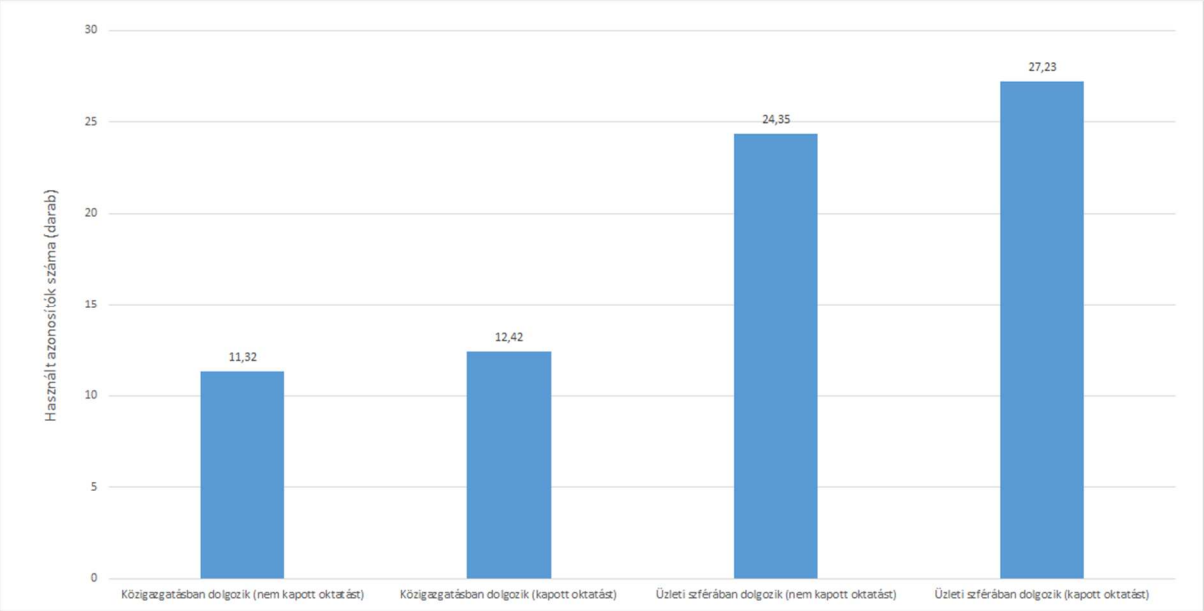
közig minta, az oktatást kapottak: azonosítók száma: 12,42 jelszavak száma: 10,31
közig minta, oktatást nem kapottak: azonosítók száma: 10,18 jelszavak száma: 8,66
teljes mintán az oktatást kapottak: azonosítók száma: 17,11 jelszavak száma: 13,52
teljes mintán oktatást nem kapottak azonosítók száma: 14,72 jelszavak száma: 12,39

Az egyértelműen kirajzolódik, hogy a jelszavak és az egyes különböző rendszerek számossága eltérő. Így feltételezhető, hogy újrahasználják a jelszavakat, több rendszerhez is ugyanazt, vagy nagyon hasonlót.

Ugyanakkor érdemes megvizsgálni, hogy ezel párhuzamosan változik-e a használt információs rendszerek száma és milyen mértékben.

A 2.37 Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.) kérdésre közigazgatási mintán 11,32 az átlagos darabszám, akik közig és oktatást kaptak az átlag 12,42-re emelkedik. Azaz megállapítható, hogy kevesebb a jelszavak száma, mint a használt információs rendszerek száma. Az oktatást nem kapottaknál 17,5%-al magasabb a rendszerek száma a jelszavak számánál, az oktatást kapottaknál kicsit mérsékeltebb 16,9% -al magasabb a rendszerek száma a jelszavak számánál.

A 2.37 Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.) kérdésre az Üzleti szférában vizsgálva az előbbieket a teljes mintán 24,35 az átlagos darabszám. Amely mindössze 3,81 %-os növekményt jelent. Míg az üzleti szférában oktatást kapottak 27,23 az átlagos szám. A jelszó és információs rendszerek számosságának százalékos eltérésére így 12,44% adódik, amely alacsonyabb, mint ugyanezen szempontok szerint a közigazgatási mintán vizsgált értékek.



62. ábra: : "Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?" kérdésre adott válaszok, forrás: saját szerkesztés

Bármelyik jelszavadra igaz-e, hogy...

2.38 ...csak betűket tartalmaz!

teljes mintán: 24,93% teljes mintán oktatással: 24,71%, közig mintán: 20,57%, mig közig mintán oktatással: 19,73%

2.39 ...betűket és számokat is tartalmaz!

teljes mintán: 78,68%, teljes mintán oktatással: 77,07%, közig mintán: 77,08%, mig közig mintán oktatással: 75,65%.

2.40 ...betűket, számokat és speciális karaktereket is tartalmaz

teljes mintán: 55,67% , teljes mintán oktatással: 60,22%, közig mintán: 46,87%, mig közig mintán oktatással: 48,68%.

Ez a pont kiértékelés során az látható, hogy a közigazgatási mintán a 2.40-es kérdés tekintetében mind oktatással, mind az oktatás nélküli csoportot véve alacsonyabb a százalék a közigazgatási csoportban, mint a teljes mintában.

A teljes mintán (1243) vizsgálva, 837 fő válaszolta, 67,3% hogy tudja valamely ismerősének legalább egy jelszavát. Ha a teljes mintát az oktatásban részesültekre szűrjük (445), akkor ez (318 főre) 71,46%-ra növekszik, egyébként elsőre meglepő módon. Ha ugyen ezen elemzést futtatjuk le a közigazgatási mintán, akkor a teljes közig mintán (384) vizsgálva (219) 57,03% állítja, míg az oktatásban részesültekre tovább szűkítve érdekes módon itt is minimális emelkedés tapasztalható 58,55%. Az inverz változás megértéséhez pontosan a H1 nyújt segítséget, azaz ahogy már disszertációmban kifejtettem a szabályzatok kialakítása csak az érintettek bevonásával, a munkafolyamatok megértésével és azokban való alkalmazhatóságának megvizsgálásával jöhetne létre hatékonyan. Ennek elmulasztásával jellemzően együtt jár a kétirányú csatorna hiánya, azaz a szabályzat habár elérhető lehet, de nem értelmezhető, nem alkalmazható a munkavállaló által. Ugyanez a érvényes az információbiztonsági tudatossági oktatás esetében, az online, visszacsatolási lehetőséget, nem tartalmazó, bevonódást lehetővé nem tévő oktatás, nem képes kiváltani a várt gyakorlatba átültetés eredményét, a jelenléti oktatás szükségességét támasztja alá, annak hatékonyságát az írásbeli szabályozás mellett. Hiszen, habár az előző kérdésekre adott válaszokból kiderült, hogy tudják, tisztában vannak az elvárásokkal, törekszenek is azok betartására, azonban rendkívül magas százalékban sértenek alapvető szabályokat és nem csak megadják, de ők is tudják más jelszavait, azaz érvényesül a csoportnyomás, racionalizálás. Továbbá, az oktatás sem jelent megoldást ennek a gyakorlatnak a csökkentésére, hiszen az oktatottak körében mind a teljes mintán, mind pedig a közig mintán emelkedés tapasztalható a rossz gyakorlat tekintetében.

2.50 Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz? kérdésre a teljes mintából 1113 fő válaszolt erre a kérdésre, melynek átlaga 3,28 egy 6 fokozatú skálán. Az oktatást kapottakon belül ez az érték 3,24-re csökkent, tehát kevésbé valószínű, hogy az új jelszó köthető a régihez.

A közigazgatásban ez az érték 3,29, azaz magasabb, amely jelen esetben “rosszabb”, mert valószínűbb, hogy az új jelszó köthető a régihez. A közigazgatásban oktatásban részesülőknél ez az érték 3.37 ami érdekes jelenség, hiszen arra enged következtetni, hogy valamilyen nehézség vagy tudáshiány állhat az egyértelmű biztonsági ajánlással szembemenő gyakorlat mögött. Amely viszont arra utal, hogy lemaradást tapasztalható a közigazgatási területen.

Ezt követően indexet képeztem az alábbi kérdésekre adott válaszokból és csoportosítási változónak a Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? kérdést állítottam be.

1. Hozzávetőlegesen hány darab különböző jelszót használsz?
2. Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?
3. Milyen sűrűn változtatod meg (általában) a jelszavaidat?
4. Hány karakter a leghosszabb jelszavad?

5. Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?
6. Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?

Majd Mann-Whitney Testnek vetettem alá ezen értékeket. Az üzleti szférában csak az azonosítók számában igazolható jelentős eltérés (M-W: Z=-3.028, p=0.002) az oktatásban részesült és abban nem részesült dolgozók között: az oktatásban részesültek jelentősen nagyobb számú azonosítóval rendelkeznek.

A közszféra esetében azonosítók számán kívül a jelszavak számában is kimutatható jelentős eltérés az oktatásban részesültek és abban nem részesültek között: itt is az üzleti szférához hasonlóan az oktatásban részesültek jelentősen nagyobb számú jelszóval és azonosítóval rendelkeznek.

Az oktatás hatását további kérdésekre is megvizsgáltam, így a Van-e olyan jelszavad, ami tartalmaz személynevet?, szféra szerint az oktatás függvényében vizsgálva azt az eredményt kaptam a khi-négyzet próba eredménye ($p>0.05$) nem szignifikáns, így nem igazolható jelentős eltérés az oktatásban részesültek és nem részesültek között a személynevet tartalmazó jelszó használatának gyakoriságában, sem az üzleti, sem a közszféra esetében.

Valamint a Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul? kérdésre is vizsgálva, hasonló eredményt kaptam, amely a minta jóságát mutatja, együtt mozogtak ezen változók. A khi-négyzet próba eredménye ($p>0.05$) nem szignifikáns, így nem igazolható jelentős eltérés az oktatásban részesültek és nem részesültek között abban, hogy van-e olyan szó, név, kifejezés, amelyik több jelszóban is előfordul, sem az üzleti, sem a közszféra esetében.

Véleményem szerint a fenti két kérdésre kapott statisztikai próba eredményének az lehet az oka, hogy habár kaptak oktatást, de az oktatás nem terjedhetett ki sok esetben a jelszóképzési gyakorlatra, hanem azt feltételezem, hogy a ‘klasszikus’ használ jó hosszú, használj jó jelszót szabályismertetésre csak. tehát a szabályalkalmazás gyakorlati megvalósításához nem kaphattak elegendő ismeretanyagot. Ezt az elméletemet a saját nagyszámú oktatási tapasztalatom, valamint Szász – Kiss kutatása is alátámasztja Hiszen ott a szabályalkalmazásra fókuszáló oktatásnál a csoport 68,4%-a a hosszabb jelszavakat kezdett használni.

4.2.2. KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI KÉRDŐÍV ELEMZÉSE

A tudatossági oktatás (viszonylag) sűrű, rendszeres, periodikus megtartását támasztja alá a következő kérdéscsokor elemzése. E szempontból különösen indikatívnak érezzük, ezért részletesen is megvizsgáljuk a következő kérdésre adott válaszokat: Használhatja ön saját mobil

infokommunikációs eszközeit (pl. okos telefon) céges információk tárolására és átvitelére? Azért különösen fontos ez a kérdés, hiszen két oldalról is veszélyforrást jelent: egyrészt a céges adat saját (magán) adathordozóra kerül és ott veszélyeknek van kitéve, másrészt a magán adathordozó bekerül a céges hálózatba, ahol ebből adódóan szintén károk keletkezhetnek.

- A válaszadók 17,4%-a felelt igennel erre a kérdésre. Esetükben a szoftverfrissítések és hardvercserék, illetve úgy általában a változások okán javasolt időközönként a felhasználók oktatása, szinten tartása, az esetleges incidensek tapasztalatainak visszacsatolása.
- A válaszadók közel 43%-a nemmel felelt erre a kérdésre. Márpedig a tiltás alapvetően nem az egyetlen jó megoldás. Ennek oka, hogy kerülőutak keletkezhetnek. A munkavállaló kifejezetten kényelmetlennek érezheti a helyzetet, nem ért egyet a szabályozással és úgy érzi, hátráltatja a munkáját. Hosszú távon pedig, amennyiben megengedőbb irányba változik a céges szabályozás, akkor ezt a szegmenst teljesen nulláról kell majd oktatni. A korlátozás – tiltás kivitelezése a technikai támogatás formájában kell, hogy jelentkezzen. A technikai tiltásra vonatkozó szabályozást transzparens módon érthetővé kell tenni az informatikai szabályzatban, világosan rámutatva, hogy miért szolgálja a biztonság és hatékonyság érdekeit.
- A válaszadók 21%-ára igaz, hogy a cég által nyújtott szolgáltatás igénybevétele esetén használja ezeket az eszközöket. Ez a körülmény, habár szakmai szempontból ideális, a teljes használhatósággal együtt is kisebb arányban van jelen, mindössze 40%-ban. Ha egy szolgáltatás jól meghatározott, körülhatárolt, az nagyban segíti az alkalmazottak életét és munkavégzését. Az effajta visszajelzések indokolhatják a szolgáltatások módosítását.
- Az első kategóriával csaknem egyező arányban (18,7%) feleltek a megkérdezettek „Nem tudom.” válasszal az adott kérdésre. Ez a válasz leginkább abban az esetben fordul elő, amikor a munkavállalók első alkalommal rendelkeznek a céges adatvagyonához csatlakozni képes informatikai eszközzel, illetve amikor első ízben értesülnek a hozzáférés lehetőségéről. Csaknem minden ötödik munkavállaló jelent ilyen kockázati tényezőt a szervezet adatvagyonára nézve.
- Egy, a biztonsági kockázatkezelés kérdéséhez hasonló kérdés vonatkozott arra, hogy mennyire jellemző különböző szoftverek letöltése a munkavégzés során. Ennél a kérésnél az arány 24%. Ezekben az esetekben nincsen protokoll arra, hogyan szükséges kezelni egy, a napi munkavégzéshez feltételezhetően valóban szükséges alkalmazást.

- A megkérdezettek 40%-a nyilatkozott úgy, hogy előfordult már, hogy lemásolta és hazavitte a céges adatvagyon valamely elemét (igaz, munkavégzési céllal, ám ez a kockázatkezelés szempontjából nem releváns).
- A válaszadók 56%-a számol be arról, hogy munkahelyén nincs érvényben vagy nem ismeri a megtekinthető weboldalakra vonatkozó előírást.
- A céges levelező rendszer tekintetében kicsit jobb az arány az előző kérdéssel kapcsolatban, ám a megkérdezetteknek még itt is 45%-a állítja, hogy nem létezik szabályozás, vagy az számára nem ismert. (Illéssy, Nemeslaki, Som, 2014)

Általánosságban elmondható, hogy megkerülhetetlen tényező lett a munkavállaló saját eszközének használata céges célokra, akár mobile device management (MDM) rendszerekkel vagy a nélkül. Ugyanakkor Miclhelberger (2020) rámutat, az MDM megoldás alkalmazásának fontosságára, a szabályozás fontosságára, a BYOD előnyeire és nem utolsó sorban a a felhasználók viselkedésének kérdéskörére. Ez is alátámasztja, hogy az információbiztonsági oktatásoknak szükséges kiterjednie a szigorúan vett munkahelyen kívülre is.

Mindezek alapján erősen javasolt az informatikai biztonsággal foglalkozó egységek megerősítése a munkaszervezeteken belül. A tudatossági képzések sokkal gyakrabban történő megtartása és sokkal komolyabban vétele. Központilag készített kérdőívvel legalább évente egyszer célszerű lenne lemérni a munkaszervezeteket annak érdekében, hogy látható, mérhető legyen az eredeti (jelen) kiindulási állapothoz mért eltérés, a várható fejlődés mértéke, adott esetben a képzés tartalmának módosítása.

Ezen kívül fontos és ajánlott a munkavállalók fluktuációjából fakadóan az új belépők oktatása a belépést követően egy viszonylag rövid intervallumon belül (pl.: 1-3 hónap). Általános szabályozási kérdés, hogy az eltérő szervezeti szabályozásokban jelenjenek meg azok a kötelező vagy javasolt elemek, amelyek minimum garanciákat jelentenek az informatikai biztonsággal foglalkozó munkavállaló jogkörére és a szervezetben arra vonatkozóan, hogy folyamatosan szinten van tartva, fejlesztve a biztonsági szint.

Számos kérdésre adott válaszban jelenik meg valamilyen tudásnak a hiánya, vagy vélelmezhető valamilyen infrastruktúrának a túlértékelése. Ezek nagymértékben ellentmondanak a vélt biztonsági szintnek. Ez vélt biztonsági szint, a vélt tudás túlértékelése önmagában is nagy kockázatot jelent, azonban itt számos tényező erősíti. Nevezetesen, a válaszadók:

- 60%-a állítja, hogy észrevenné, ha feltörnék vagy megfertőződne a számítógépe;
- 84%-a nem ért egyet azzal, hogy a vírusirtó megállít minden kártékony programot;
- 13%-a viszont nem biztos benne, hogy be van-e kapcsolva a vírusirtó a számítógépén;

- 74%-a szerint elvégzi a számítógépe a frissítések telepítését (automatikusan);
- 72%-a mondja a jelszó változtatási gyakoriságra, hogy az automata figyelmeztető üzenetekre hagyatkozik. (Illéssy, Nemeslaki, Som, 2014)

Bár ezen értékek nem teszik lehetővé általános következtetések levonását, de valószínűsítik, hogy a közigazgatás dolgozói hamis biztonságérzettel rendelkeznek, az elektronikus információbiztonság szintjét pedig rendszerint felülbecsülik, magasnak gondolják. Belső logikai ellentmondásra mutat rá például az, hogy a megkérdezettek nagy száma hagyatkozik automata frissítésekre vagy rendszerüzenetekre. Azaz jellemző, hogy a válaszadók vagy túlértékelték saját kompetenciájukat, vagy a kérdésnek megfelelni vágyva inkább pozitív választ adtak. A teljes felmérés tükrében azonban megmutatkoznak ezek az ellentmondások. Egy másik példa ilyenfajta ellentmondásra, hogy a válaszadók csaknem azonos arányban állítják azt, hogy nem bíznak meg feltétlenül a vírusirtókban, illetve azt, hogy jellemzően hagyatkoznak valamilyen automatizmusra (70%). 60% azt is állítja, hogy észlelné a vírusirtó által nem azonosított problémát is. Kisebb mértékben alátámasztja az ellentmondást az is, hogy minden nyolcadik megkérdezett (13%) bizonytalan abban, hogy fut-e a vírusirtó a gépén. (Illéssy, Nemeslaki, Som, 2014) Fontos megjegyezni, hogy a 2013. évi L. trv hatálya alá tartozó szervezetek esetében jelentős eltérés mutatkozik az informatikai infrastruktúra és az azt kiszolgáló személyzet vonatkozásában, közel sem tekinthető egységesnek. Részben ebből kifolyólag szélsőségek, eltérések tapasztalhatóak a biztonsági kérdésekben is azoknál a szervezeteknél, ahol központilag végzik az informatikai rendszerek, szoftverek frissítését nem is képzelhető el más megoldás, mint az automatizált frissítések, de az elektronikus információbiztonság szempontjából kevésbé szerencsés intézményekben ezek akár veszélyt is rejthetnek magukban.

A szervezet infrastrukturális hátterére vonatkozólag pozitív attitűd tapasztalható, bíznak a rendszerben, a vélhetően központi szabályozásban vagy az előírásokban. Bár láthatóan az előírásokkal pontosan, egzakt módon nincsenek tisztában (kiragadott példa az előzőekben már sok fel volt sorolva, de 43% nem tudja, hogy a szervezetben a felhőszolgáltatás engedélyezett-e.)

Fontos megemlíteni demográfiai szempontból is, hogy bár a válaszadók zöme egyetemet, főiskolát végzett (90%), azonban jelenleg nem elterjedt informatikai biztonsággal összefüggő általános képzés. Amennyiben nem szakvégzettségről beszélünk, akkor jellemzően legfeljebb egy-két féléves általános informatikai képzésben részesültek a munkavállalók valamely munkaszervezetnél történő munkába állást megelőzően. Így a munkaszervezetekre nagy feladat és kihívás hárul, az új belépők oktatása, a régi kollégák oktatása, a folyamatos szinten tartásról való gondoskodáson túl is. Hiszen a rendszerek változásából kifolyólag, a beszállítók, partnerek, különböző kapcsolatokban is meg kell, hogy jelenjen az informatikai biztonság, ennek

tudatossága. A tudatosság különösen annak érdekében fontos, hogy az új projektek eredményeként már csak ezen elvárásoknak megfelelő implementációk keletkezzenek. Míg a meglévő rendszerek felülvizsgálata, ellenőrzése és naprakészen tartása is jó ideig munkát fog adni a területen dolgozóknak.

A képzés és az ennek eredményeként megjelenő tudatosság az egyetlen olyan elem, amely valóban hatékonyan, relatív alacsony költség ráfordítással fejleszthető, ugyanakkor folyamatosan kell is fejleszteni. A szervezet biztonsági szintjét alapvetően határozza meg a munkatársak biztonságtudatosságának szintje.

Egyes kérdések esetében javasolt lett volna további pontosító vagy ellenkérdés feltétele a jobb értelmezhetőség érdekében. Azonban ezekre a kérdőív röviden tartása miatt nem volt lehetőség. Ilyen kérdés volt például a következő: A céges informatikai rendszerbe történő bejelentkezéskor ugyanazt a jelszót használja-e, mint a személyes célokra fenntartott fiókjai esetében? Itt pontosító kérdésekkel kideríthető lenne, hogy a magánszférában használt jelszavai különböznek-e. Vagy, hogy a céges jelszavak különbözősége szabállyal van-e kikényszerítve, vagy a tudatosságból fakad. Továbbá technikai részről fontos lenne tisztázni, hogy mit értünk egyezőségen és különbségen. Mivel az egyetlen karakterben különböző vagy más szempontból könnyen visszafejthető jelszavak nem teljesítik a megfelelő biztonsági követelményeket.

Pozitív eredmény ugyanakkor, hogy a megkérdezettek 80%-a még nem jelentkezett be a céges informatikai rendszerbe valamilyen nyilvános számítógépről. Ez nagyon jó eredménynek számít, de a valós okokra nem világít rá. Lehet, hogy a munkaszervezet nem biztosít ilyen lehetőségeket, vagy tiltva van, vagy csak egyszerűen nem végez távolról munkát, tehát nem derül ki, hogy szabályozás, képzés vagy infrastrukturális okok miatt jött ki ilyen magas eredmény.

A kérdőív nagyon jól kimutatja azokat a neuralgikus területeket, amelyek alapján láthatóvá váltak az ellentmondások. A válaszadók nagyon, mondhatni talán túlzottan is magabiztosak saját tudásokban az általuk használt rendszerekben. Ezzel párhuzamosan tetten érhető a kérdéseknek, kérdőívnek való megfelelési szándék, ez szerencsére a referencia kérdésekkel kimutathatóvá vált.

A kérdőív és a szakértői interjúk alapján javasolt központilag kiadni olyan általános segítséget, amelyet adott területen tevékenykedő szervezetek be tudnak építeni a saját szabályozásukba. (Az éves kérdőíves felmérésekhez is javasolt ilyen központi ajánlás kiadása, vagy legalább a mérendő területek megnevezése az ajánlásban.)

Így hosszú távon az elektronikus informatikai biztonságra vonatkozó belső szabályozások közelednének egymáshoz, nagyobb összhang lenne teremthető közöttük. A szervezeti elektronikus információbiztonság egyenszilárdsághoz minden egyes munkavállalót el kell tudni érni az oktatással. Olyan komplex képzési tematika kialakításával, amelyben az elektronikus

információbiztonsághoz szorosabban vagy lazábban kötődő területek szempontjai is megjelennek. Nyilvánvaló ugyanis, ha valaki kinyomtat egy fontos dokumentumot, az abban tárolt információk védelme ugyanolyan fontos, mint valamilyen adathordozón tárolt formájában. Lehetővé és kötelezővé tenni a részvételt. A közszférában párhuzamosan meginduló ilyen jellegű képzések (központilag kiadott segítséggel, ajánlással) jelentős szinergikus, egymást erősítő, támogató hatásokat tudnának generálni, a részek összessége több lenne, mint elszigetelt, szeparált képzések esetén.

A kérdőív nem csak megmutatta az ellentmondásokat, hanem sikeresen feltárta az ellentmondások okait is. A szervezeti tudás érzékelhetően túlértékelt, a tisztázó kérdésekre adott válaszok eredményeinek tükrében azok valós tartalma esetleges, bizonytalan. Az informatikai biztonsági egységek szervezeten belüli hierarchia szintje a javasoltnál alacsonyabb, vagy nem létezik, sok esetben keverik vagy összemossák az általános, üzemeltetési informatikával.

4.2.3. KÖZIGAZGATÁSI INFORMÁCIÓBIZTONSÁGI INTERJÚK ELEMZÉSE

Egybehangzó szakértői vélemények, az interjúk alapján ugyanakkor egyrészt közigazgatási rendszereink heterogenitása és decentralizáltsága, valamint a nehezen belátható költséghatékonyság javulás miatt továbbra is lemaradásban leszünk, amennyiben ezeken a területeken nem történik szisztematikus építkezés. Interjúink megerősítik, hogy ezen nagymértékben segíthet az információbiztonsággal kapcsolatos humán erőforrás-fejlesztés információbiztonsági vezetői és alkalmazotti szinteken is. Az információbiztonság vonatkozásában egyértelmű az egyetértés az egymás közötti kommunikáció hangsúlyozásában, a pontos egyéni és szervezetek közötti felelősség meghatározásában, a viselkedés és a kultúra meghonosításában; azaz nem elsősorban a technikai, hanem a humán területek húzó hatásának kihasználásában. Ez a logika egyébként nagyban összecseng azokkal az innováció befogadási paradigmákkal, amelyek megmutatják a szervezeti és human abszorpciós képességeket, amelyek nélkül nem kerülnek befogadásra a technológiai innovációk. Ebben a vonatkozásban, tanulmányukban felhívtuk a figyelmet a szereplők heterogén szakmai alapjaira, tudására és motivációjára. (Illéssy, Nemeslaki, Som, 2014)

A képzés azért kiemelten fontos, mert ezzel a negyedik szinten, vagyis a közigazgatás munkahelyeinek a szintjén teremtődik meg egy olyan szakmai alapja az elektronikus információbiztonságnak, amelyeken keresztül a felsőbb szinteken elindított folyamatok sokkal gyorsabban és hatékonyabban tudnak beszivárogni a mindennapi munkavégzés rutinjába. Létező probléma, hogy ha fel is tárnak valamilyen biztonsági hiányosságot egy adott munkahelyen,

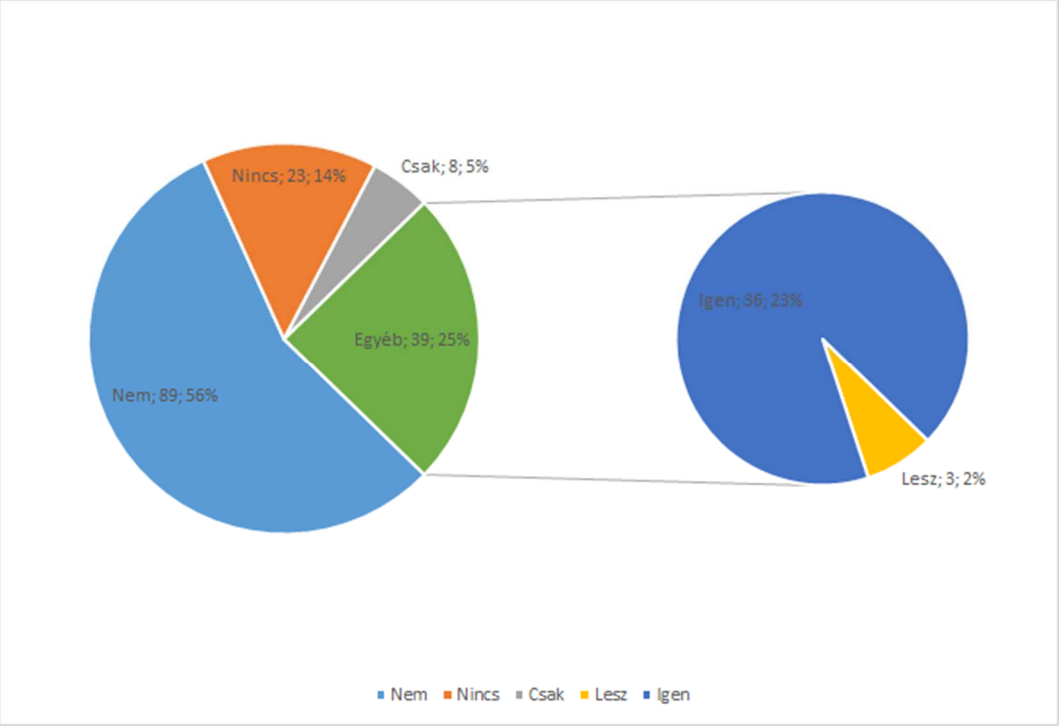
évekig nem javítják ki, mert nem tudják, miért fontos, nem érzik magukénak. Az EIB-felelősök feladata lesz az EIB ügyének képviselete a munkahelyeken. Szintén fontos, hogy a különböző intézményeknél dolgozó EIB-felelősök között kialakuljon egy szakmai párbeszéd, de erről a későbbiekben szólunk majd.

4.2.4. INFORMÁCIÓBIZTONSÁGI SZAKEMBER KÉRDŐÍV ELEMZÉSE

Az „Ön munkaszervezetében dolgozók száma? (Akik információbiztonsági szempontból az oktatandók!) 2 db szám?" kérdésre átlagosan több száz fős létszámokat adtak meg, azaz egyes munkaszervezetekben ezres létszámmal vannak jelen információbiztonsági szempontból oktatandók.

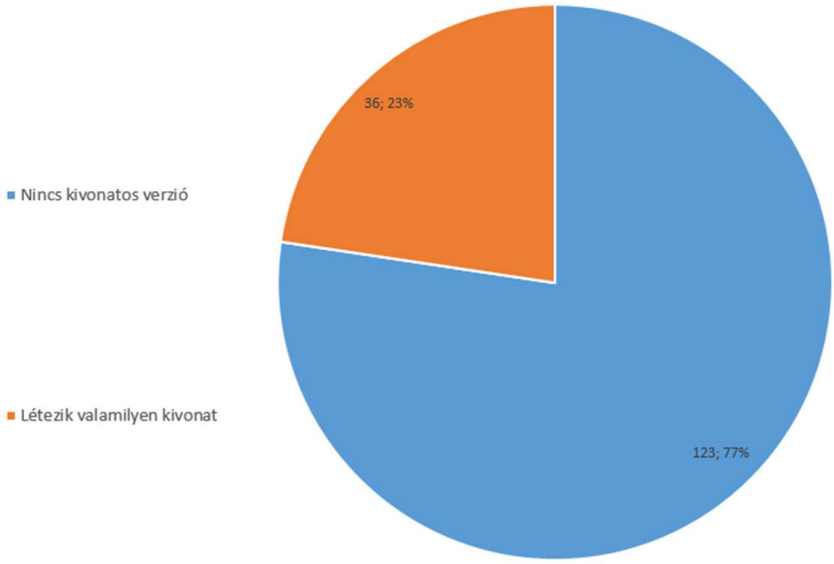
„Tartott-e már a munkaszervezetben információbiztonsági oktatást? Tapasztalatok / mikorra és hogyan tervezi / elképzelések a megvalósításról?" kérdések feltevésre kerültek. Ezen kérdésekre adott válaszokból az látszódott, hogy túlnyomórészt ilyen oktatást még nem tartottak.

A 27. Az információbiztonsági szabályzatnak létezik-e kivonata, kivonatos verziója? kérdésre adott szabadszavas válaszokat szógyakoriság elemzéssel vizsgáltam, természetesen a tételes áttekintést mellett. A nemleges válaszokat, tehát ahol az adott IBSZ-nek nem létezik szerepkör alapú, vagy rövidített, kivonatos verziója, egyesével is vizsgáltam, hogy milyen megfogalmazást alkalmaztak. Ahol az igen mellett a lesz, el fog készülni utalás szerepelt, azt is az igen csoportba soroltam az alábbi ábrán.



63. ábra: "Az információbiztonsági szabályzatnak létezik-e kivonata, kivonatos verziója?" kérdésre adott szabadszavas válaszok szógyakorisága, forrás: saját szerkesztés

Egybevonva azon csoportokat ahol jelenleg nem létezik kivonat az IBSZ-ből összességében 75%-a a megkérdezetteknek így nyilatkozott. Amit azért is tartok roppant pontos és reprezentatív mintának, mivel jelenleg és a jövőben is ilyen területen, konkrétan ezen szabályzattal dolgozó, azt ismerők nyilatkozták.

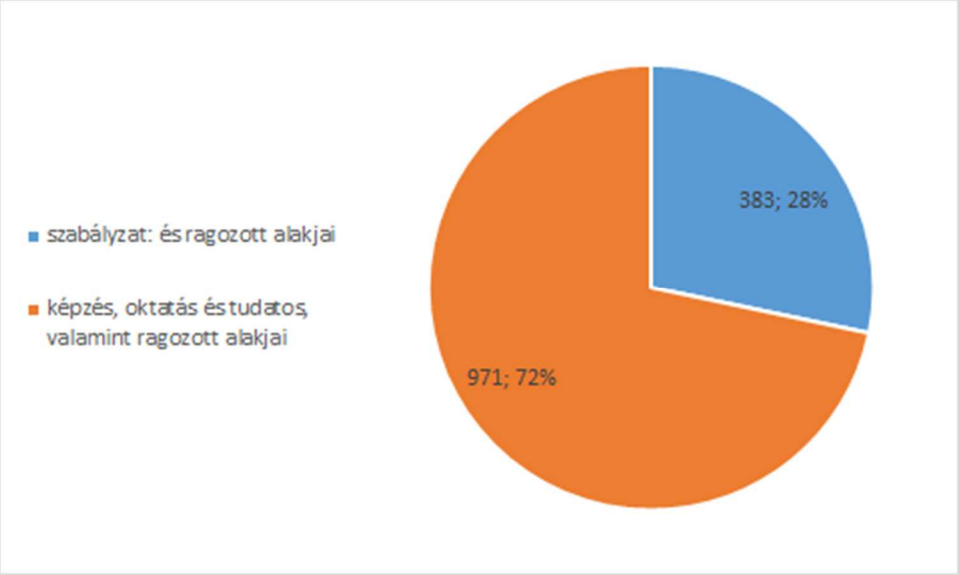


64. ábra: Annak aránya ahol az információbiztonsági szabályzatnak jelenleg létezik-e kivonata Forrás saját szerkesztés

Ha a kérdést teljes szigorúsággal vizsgáljuk, hogy jelenleg mi az ami már elkészült, akkor ez az arány még rosszabb 77%-23% -ban oszlik meg, és a többségnél nem létezik kivonat ez látható a 64. számú ábrán.

A teljes mintában és az összes válaszban vizsgálva érdekes megfigyelni, hogy habár az információbiztonsági elvárt viselkedés alapján a szabályzat alkotja, az alábbi szavak használatának gyakorisága azt mutatja, hogy az információbiztonsági szakemberek szerint fontos a képzés, oktatás

oktatás és ragozott alakjai: 345
képzés és ragozott alakjai: 349
szabályzat: és ragozott alakjai: 383
tudatos és ragozott alakjai: 277
darabszor fordulnak elő.



65. ábra: Képzés fontosságának megítélése, nem direkt kérdésként feltéve a válaszok szóhasználata alapján, az információbiztonsági szakemberek körében, forrás: saját szerkesztés

Voltaképpen is megjelenik roppant láthatóan és transzparensen, hogy a megkérdezett információbiztonsági szakemberek hogyan súlyozzák a szabályzat és a képzés viszonyát.

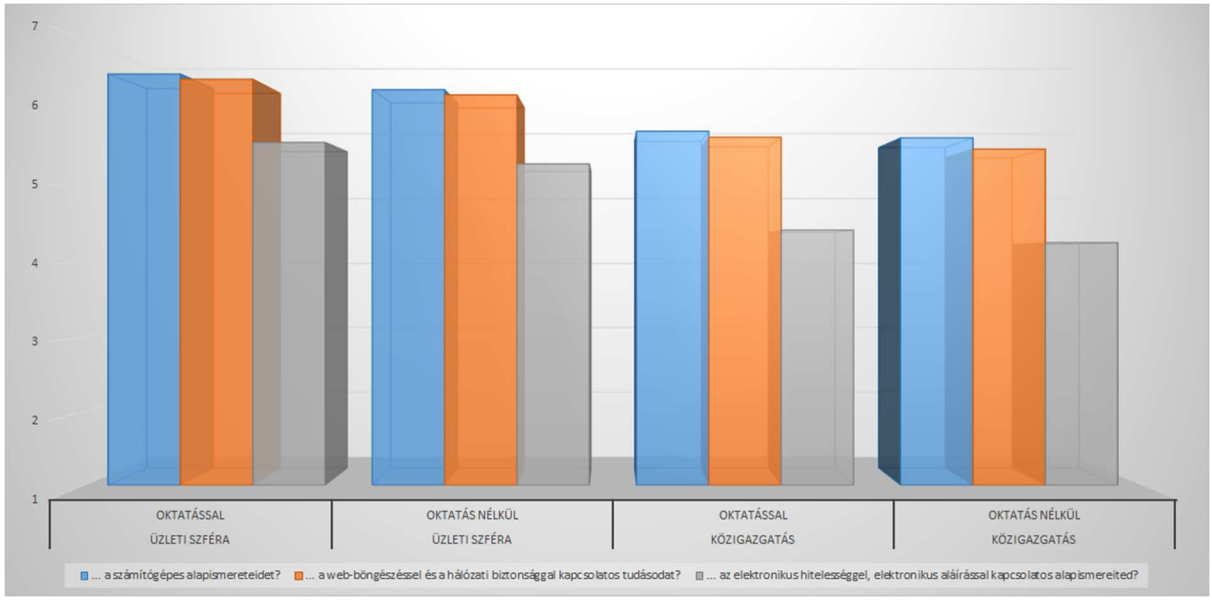
Ezt követően azt vizsgáltam meg, hogy az IKT képességekre vonatkozó kérdésekből képzett indexek mennyiben függnek össze. (14. sz. táblázat)

	Üzleti szféra oktatással	Üzleti szféra oktatás nélkül	Közigazgatás oktatással	Közigazgatás oktatás nélkül
... a számítógépes alapismereteidet?	6,55	6,34	5,78	5,69
... a web-böngészéssel és a ***hálózati biztonsággal kapcsolatos*** tudásodat?	6,48	6,27	5,7	5,54
... az elektronikus hitelességgel, elektronikus aláírással kapcsolatos alapismereited?	5,63	5,34	4,45	4,28

12. táblázat: "Honnan szerezted ismereteidet?" kérdésre adott válaszok szférák s a kapott képzés alapján, forrás: saját szerkesztés

A 12. számú táblázatról leolvasható az üzleti és közigazgatási szféra, oktatással és oktatás nélkül adott válaszok indexált és összesített értékei. Legalacsonyabb értéket a közigazgatásban oktatásban nem részesültek adtak. Szakmailag így látható a lemaradás az egyes csoportok között és mindenképpen indokolt lehet oktatási program létrehozása.

Ezt követően azt vizsgáltam meg, szférák és oktatás szerinti csoportokban, milyen IKT képességekkel rendelkeznek az egyes csoportok saját bevallásuk szerint.



66. ábra: IKT-jártasság, ismereteid pontra adott válaszok szférák s kapott képzés alapján, forrás: saját szerkesztés

Az ábráról leolvasható, hogy a közigazgatásban, oktatás nélkül hagyott csoport minden területen bizonytalanabb tudásában, IKT-jártasságát is rendre alacsonyabbra értékeli. A mögöttes okok kapcsán felmerülhet további képzések tervezése, kifejezetten az IT rendszerek vagy alkalmazott rendszerek vonatkozásában.

4.2.5. KÖZIGAZGATÁSI KÉPZÉS ELŐTT/UTÁN KÉRDŐÍV ELEMZÉSE

Az oktatás előtti kérdőív kiértékelése

Az 1. Hallott-e már régebben EU Safer Internet Programjáról? kérdésre 6 fő válaszolta azt, hogy "Talán, már hallottam róla", míg 18 fő azt, hogy: nem. Az EU Safer Internet Program egy, az egész Európai Unióra kiterjedő kezdeményezés amely 2009 óta elérhető Magyarországon is. Önkéntes oktatók segítségével bármelyik Magyarországi általános vagy középiskolába díjmentesen kérhető információbiztonsági előadás, oktatás.

Ez a 12. Ön miért döntött ezen oktatáson való részvétel mellett? kérdéssel összevetve 13 fő adott olyan választ, hogy gyermekével, vagy családtagjával kapcsolatos motiváció miatt vesz részt az előadáson, kíváncsi annak tartalmára.

Az 4. Napi hány órát használja az internetet gyermeke? kérdésre átlagosan 1,83 óra volt a válaszok.

Több előnye vagy több hátránya van az "internet használatának" ön szerint? 23 fő azt mondta, hogy inkább több előnye van, míg egy fő válaszolta, hogy inkább több hátránya van. A 6. Mennyire tartja hasznosnak az internetet a mai világban? kérdésre adott válaszok átlaga 7,96 volt egy tíz fokozatú skálán.

A 10. Tudta-e Ön, hogy a Safer Internet ingyenes képzéseket tart? kérdésre, amely a tanulásra való hajlandóságot, az információbiztonsági tudásra való nyitottságot vizsgálta a válaszadók mindegyike azt választotta, hogy "Nem, de élnék a lehetőséggel".

És végül a 11. Ön szerint hány oldal terjedelmű az informatikai szabályzat? kérdésre, a 10 oldal és 150 oldal között lehetett választani 8 lehetőség közül. Helyes választ 3 választ mindössze 3 fő adott, mivel a szervezet akkor hatályos IBSZ-e 107 oldal terjedelmű volt.

A szervezetnél nem alkalmaztak (ezt megelőzően egyetlen egyszer sem) tantermi oktatást, hanem a szabályzatot tették elérhetővé az intraneten. És az éves kötelező vizsga is az intranet oldalon volt elérhető. A vizsga fix kérdéseket tartalmazott, azaz a kérdések és helyes válaszok mindenkinél azonosak voltak a munkaszervezetben.

Mindezek alapján arra lehet következtetni, hogy mivel a munkavállalók az információbiztonsági szabályzat hozzávetőleges nagyságát, oldalszámát se ismerik. Valamint az oktatások és személyes megfigyelés során is azt tapasztaltam, hogy annak tartalmáról, elérhetőségéről sem rendelkeznek információval, az alkalmazott pusztán online elérhetővé tétele a szabályzatnak nem jutott el a munkavállalókhoz, vagy azt nem nyitották meg, annak helyét és tartalmát nem ismerték.

Az itt ismertetett kérdések és azokra adott válaszok jól mutatják a kontrasztot, hogy valami érdekes a munkavállaló számára, felkeltette-e az érdeklődését, úgy gondolja, hogy hasznos lesz számára a magánéletben vagy munkafolyamataiban és arra minőségi és mennyiségi, dedikált időt szánt, részt vett az oktatáson. Míg az egyébként bármikor online elérhető szabályzat megismerését nem tartja fontosnak.

Disszertációmban vizsgálom az emberek motivációját, amely több tekintetben is releváns. Miért

- hajlandó időt és energiát szánni a szabályzat megismerésére,
- miért hajlandó vagy nem hajlandó szabályt szegni,
- jelenti vagy nem jelenti az adott incidenst,
- ...

A 12. Ön miért döntött ezen oktatáson való részvétel mellett? kérdésre szabadszavas válaszokat adhattak a kitöltők.

A szófelhős elemzéseknél már bemutatott műveletek végrehajtása utána az látszódik, hogy a résztvevőknél sikerült kimutatni egy speciális motivációs tényezőt.

Résztvevők kérdőíves válaszai alapján a szabadszavas mezők feldolgozása révén készült.

67. ábra: "Ön miért döntött ezen oktatáson való részvétel mellett?" kérdésre szabadszavas válaszok szófelhője, forrás: saját szerkesztés

A 67. számú ábrán a leggyakoribb szavak kerültek kiemelésre. Amely egyrészt alátámasztja, hogy a munkavállalók nyitottak az új ismeretek befogadására, akkor ha az munkafolyamataikban támogatja őket, vagy akár magánéletükben hasznos tudást biztosít. A másik fontos megfigyelés, hogy a szervezet információbiztonsági szabályzata folyamatosan rendelkezésre áll az intranet oldalon (ezt egyébként ebben a konkrét előadásomban is bemutattam), ill. természetesen az internetről is tájékozódhatnának, de mégis a személyes oktatáson való részvétel mellett döntöttek. Ez az adatok alapján, melyet megfigyeléseim is alátámasztanak egyrészt magánéleti indíttatású,

azaz látható, hogy a gyermek, a család jelenik meg motivációs tényezőként, hogy megfelelő információbiztonsági oktatást kapjon, melyet akár a magánéletben is tud hasznosítani. Másrészt az előadás után meghirdetésre került, hogy azt követően kérdés - felelek blokk is rendelkezésre áll, azaz bármilyen a témát érintő kérdést fel tudnak tenni a szakértőnek. Ebben a konkrét esetben az előadás formális lezárását követően 28 percig tettek fel mért kérdéseket az ott maradó résztvevők.

Aktív csoport esetében régóta bent tartott kérdések feltevésével egymást támogatják a csoport tagjai. Az oktató felelőssége a nyílt kommunikációra buzdítás. Amely a modellben leírt lehetséges további (szinergikus) eredményekkel járhat.

4.2.6. AZ OKTATÁS KIÉRTÉKELŐ ÖSSZEFOGLALÁSA ÉS AZ INFORMÁCIÓBIZTONSÁGI OKTATÁSI MODELL BEMUTATÁSA

Mottó:

Az 5 W+1H egy problémamegoldó módszer,
Kipling-módszerként is ismert, mivel a kérdőszavait az alábbi kis Kipling-vers foglalja össze:
"I have six honest serving men
They taught me all I knew
I call them What and Where and When
And How and Why and Who"
..
"Az elefántkölyök (részlet..
Hat őszinte szolgálót tartok,
Mindenre megtanítottak, amit csak tudok,
Neveik: Mit és Hol és Mikor
és Hogyan és Miért és Ki volt."

A modellem, valamint a modellem alapján kidolgozott mintaoktatásom, amelyet nagyságrendileg 2010 óta folyamatosan fejlesztek, több száz információbiztonsági óra megtartása során jelenleg is fejlődik a kutatásaim, megfigyeléseim és a visszajelzések alapján. Összességében több, mint hatezer résztvevő számára tartottam meg ezen előadást. Valamint ezen modellt figyelembe véve e-learning oktatások több mint négyezer fő részvételével kerültek elvégzésre. Szerencsémre nem csak a Nemzeti Közszolgálati Egyetem, Elektronikus információbiztonsági vezető szakirányú továbbképzési szakon tanulmányokat folytató információbiztonsági vezetőknek volt lehetőségem ezen oktatások megtartására, hanem számos szervezetnél az EU SIP keretében, Hivatalok Napja, Nyitott Bíróság, vagy a Polgári Igazságszolgáltatás Európai Napján, stb. hozzávetőlegesen 10 évestől korosztálytól kezdve változatos életkorú és eltérő profilú munkaszervezetekben dolgozó munkavállalók részére is.

A disszertációmhoz is becsatolt előadások egyike az alábbi megfontolások alapján nyerte el jelenlegi formáját a 2010 óta tartó fejlesztés során. Az alábbi táblázat, ábra a módszertani blokk bemutatását tartalmazza, annak jobb megértését szolgálja.

Cél	Eszköz	Módszer	Egyéb
Kockázatokra reagálás, kockázatarányos oktatás	Adott szerepkörre való felkészülés. (Munkafolyamatok ismerete, szerepkörre illeszkedő életszerű példák.)	Szerepkör alapú oktatás. Sortlist az üzenetekből.	Előzetesen a kockázatok felmérése, szervezet vagy munkakör alapján.
Szabályzatkövetési hajlandóság növelése	Jelenlévők bevonásával élő demo.	Az egyes kockázatokra munkafolyamatból és/vagy magán / héköznapi életből vett példa, demo bemutatása.	A megcélzott shortlistes területen azonosított kockázatokra adott elvárt, jó reakció trenírozása, bemutatása.
Szabályzatkövetési hajlandóság növelése	Munkafolyamat és magánéleti hasonlóságok összekötése.	A bemutatott demo rövid értelmezése.	Megbeszélés. Kérdésfeltevéssel.
Szabályzatkövetési hajlandóság növelése	Szabályzat pár mondatos ismertetése.	Visszacsatolás, megerősítés, összefoglalás.	Áttekintés: Kockázat Jó és rossz viselkedési minta. Lehetséges következmények áttekintése a demo után.
Szabályzatkövetési hajlandóság növelése	Kérdések, nehézségek feltárása a munkafolyamatban	Kérdések feltevésével visszacsatolást kérni, hogyan tudják, képesek lesznek-e alkalmazni a szabályt.	Azon visszajelzéseket rögzíteni kell, amelyek csak szabályzatszegéssel, vagy más előírt módon nem végezhetőek el.

13. táblázat: Az oktatás módszertani összegzése, forrás: saját szerkesztés

További fontosabb megfontolások a tervezés és kivitelezés során megfontolásuk az alkalmazhatóság függvényében javasolt:

- Legyen érdekes: Star Wars, képregény, vagy valamilyen történet, gondolati ív. (Fontos, hogy ne csak hasznos, de szórakoztató, érdekes is legyen az átadott információ, vagy annak az átadási formája.) “Tudományos érdekesség”: 10 utolsó bankkártya tranzakció, jelszó visszafejtés.

- Kérdések feltevése: A kérdések feltevése segíti a bevonódást. Valamint visszacsatolást is ad az aktivitásról, a gondolatokról, a szabály alkalmazhatóságáról. az információbiztonsági szakterület a kapott visszajelzéseket dolgozza fel.
- Helyi, élő bemutatóval támogatott (demo) előadás, a jelenlévők bevonásával. Egy vagy több önként jelentkező résztvevő bevonása. (például: egyik résztvevő által beírt jelszó visszafejtése, feltörése; bankkártya elkérése abból információ kiolvasása, bankkártya CVC kód megszerzése, mini kamera kézbe adása, mini kamerával történő információszerzésre bemutató példa, stb.)
- Folyamatos reagálás és dinamikus módosítás a visszajelzések, kérdések alapján. Az ismertető frontális blokkok megszakítása legalább 10-15 percenként. Visszakérdezés, aktivizálása.
- Pozitív visszacsatolások, jutalmak, elismerések, oklevelek az információbiztonsági jó teljesítményért, szabálykövetésért, stb. Ennek alkalmazása az előadás során és végén. (Például: Star Wars pecsét, Star Wars-os designú cukorka, oklevél, részvételi igazolás, egyéb.)
- Lépjünk ki a "csak a munkaszervezeti" kérdések megközelítésből. Bátran mutassuk be, hogy ezt így javasolt csinálni a magánéletben is, de ott nem tudjuk ugyanezt a biztonsági színvonalat garantálni, épp ezért fontos Neked követni az előírásokat.

Oktatási szint dimenziójával kapcsolatos megfontolások:

- alapvető jelenállapot mérés, kiértékelés,
- alapvető jelenállapot információbiztonsági oktatás, és teszt/vizsga
- szerepkör alapú oktatást megelőző mérés, szerepkörönként,
- szerepkör alapú, adott szerepkörre szabott jelenállapottal összefüggő belépő szintű információbiztonsági oktatás, és teszt/vizsga
- éves ismétlő oktatás, éves ismétlő mérés,
- adott eseményhez (kiberhónap) vagy adott incidenshez, vagy támadási vektor változáshoz köthető oktatás, tájékoztatás, kampány, egyéb
    - automatizált képzések terítése, amennyiben lehetséges,
- bevonódást, kötődést célzó kommunikáció (vicces, szórakoztató, de releváns tartalmak, érdekességek)
- visszacsatolások, eredményesség mérések.
- további szervezet, szerepkör, vagy üzenetspecifikus megfontolások.

Az időbeli elterítés alkalmazása adott munkaszervezeten belül és annak előnyei

A mozaikmódszer, elsősorban nagyobb munkaszervezetekben alkalmazható hatékonyan, pár tucat fős munkaszervezetekben vélhetőleg nem életszerű a kivitelezése. Ennek lényege, hogy az információbiztonsági oktatási stratégiához illeszkedve, az éves terv végrehajtása során figyelembe lehet és kell venni a csoportnyomás, az informális csatornák jelentette hatásokat is, azt az információbiztonsági oktatás, szabály-alkalmazási hajlandóság és gyakorlat szolgálatába kell állítani, tervezetten. Például: legyen az "A" szervezet főigazgatóságai I., II., III,... m. Legyen

az azon szervezeti egységekben dolgozó munkavállalók jelölése így a I.1, I.2, … I.n … II.1, II.2., … II.n, ..., m.n. jelölés alkalmazható.

Ezt a jelölést alkalmazva minden olyan szervezeti egységre (I, II, ... m.), amelyek létszáma eléri a meghatározott főt, nem szervezeti egységenként történik meg az oktatási (vagy felejtési görbe lefutását befolyásoló tevékenységek kivitelezése) tevékenység, hanem szervezeti egységen belül időbeli eltolást alkalmazva.

Például:

Március első fele: I.1, I.3, I.5, … I.n / 2+1. és II.1, II.3, II.5, … II.n / 2+1… Azaz kimaradtak az oktatás első periódusából a I. számú szervezeti egység I.2, I.4, ... I.2n és II.2, II.4, II.2n, stb. munkavállalói. Természetesen másféle rotáció is elképzelhető amely képes megvalósítani, hogy szervezeti egységeken belül indukálja a kommunikációt információbiztonsági témakörben, abban az esetben is, ha X, (ahol X>3) munkavállaló esetén X ε (x1,x2,x3, ...xn) esetén legfeljebb X halmaz számosságának egy bizonyos 50%-nál kisebb része került az adott periódusban képzésre beiratva.

Azaz az egyes szervezeti egységek között is alkalmazható a mozaikmódszer, időbeli eltolás, valamint a szervezeti egységeken belül is javasolt ennek megtervezése.

Így voltaképpen akár heteken, hónapokon keresztül fog futni, futhat egy adott. például jelszóbiztonsági kampány. Előnye, hogy az informális csatornákon, a hétköznapi kommunikációban az egyébként egyszer impulzus széthúzódik és akár több hónapra elterül.

A modell látszólagos egyszerűsége mellett fel kívánom hívni a figyelmet, hogy az éves képzési program elindításakor, annak elején szükséges az összes tényező meghatározása. A tervezéskor javasolt az összes kérdés megválaszolása. Például a tervezéskor, még az indulás előtt érdemes a mérési módszert is meghatározni, az abból (tervezés során szimulált) kieső eredmények felhasználhatóságának validálása. Ha szükséges a tervezés pontosítása. Természetesen lehet kisebb módosításokat végrehajtani és szükséges is lehet, de fontos, hogy a teljes kép legyen meg az induláskor. Az éves (általános) képzési tervet is érdemes figyelembe venni a szervezeti stratégiai célkitűzésekhez igazítva.

Összegezve, a kockázatokra reagálva, azoknak a tipizálható jegyeire is ki kell, hogy terjedjen a felkészítés, természetesen kockázatokkal arányosan, eltérő mértékben. Ennek megfelelően ésszerű egységekre osztva az egyes témakörökre a gyakorlatban tapasztalt mintákkal (azok felismerését támogatva) kell hasznos gyakorlatorientált támogatást biztosítani.

A oktatás hatásfokáról pedig meghatározott időn belüli teszteléssel lehet jól megbizonyosodni. Amikor is nem kérdéslista, tehát nem elméleti, hanem gyakorlati tudás mérésére javasolt fókuszálni.

A felismerhető, tipizálható jegyeket, az egyes kockázatokra, visszaélés típusokra reagálva fel kell, hogy ismerje a munkavállaló. Ekkor lehet mérni, hogy mennyire követi az előírt protokollt, például.:

- megnyitja-e a phishing teszt levelet,
- kattint-e a benne lévő linkre,
- megadja-e a jelszavát,
- törli-e a levelet és nem jelenti be,
- nem nyitja meg és bejelenti a levelet,

pár a lehetséges és tipizálható viselkedési mintákból, amely részben modellem lényege, hogy oktatás (tréning) során a felismeréshez és javasolt műveletsorhoz szükséges összes tudást és egyszeri gyakorlatot is lehetővé kell tenni. Akik teszt eredménye nem tökéletes, azok számára valamilyen ismétlő oktatás előírása lehet szükséges.

A szabályalkalmazás gyakorlatára is javasolt a mozaikmódszer használata, de talán nagyobb időbeli eltolást, vagy kisebb I.10, I.20… II.10, II.20 ...m.(n / 10) mintán alkalmazva.

Javasolt a munkaszervezeti lehetőségekhez mérten az „élő" bemutatás valamint a magyarázat és a megbeszélés lehetőségét biztosítani, hogy az is megjelenjen az oktatási ciklusban. Az egyes azonosított szerepkörhöz, használathoz alkalmazkodás, példák, visszajelzés kérése, azokra reagálva folytatás

E-learning kapcsán az önálló tanulásra való sarkalás:

- csináld meg akárhányszor csak kedved tartja,
- érd el a maximális pontszámot,
- visszanézheted a kérdéseket és válaszokat,
- mindig más kérdést fogsz kapni (megfelelő nagyságú kérdésbank szükséges)

kitűző, oklevél egyéb lehetséges (e-)nyeremények lehetősége.

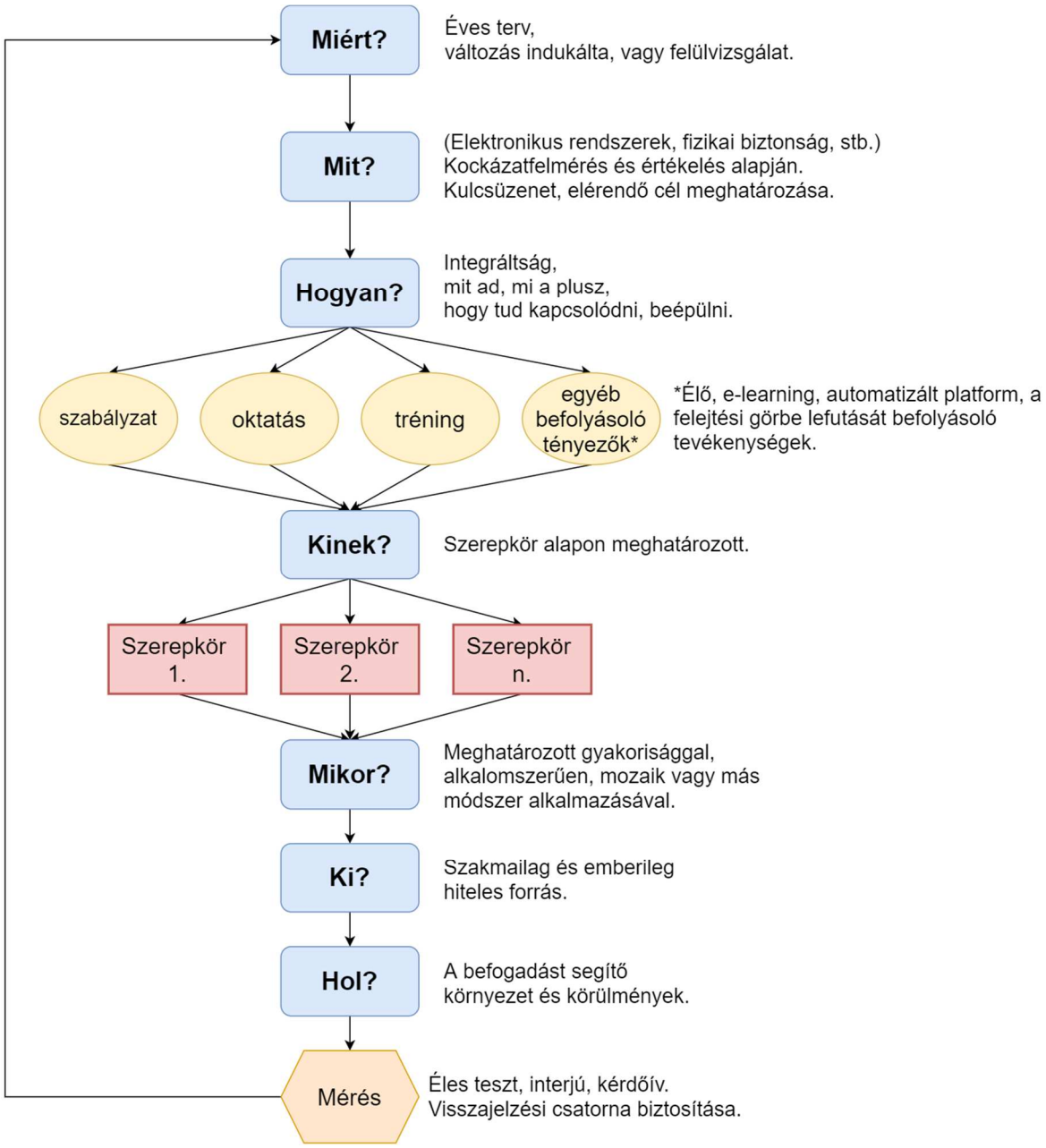
Fontos tehát, hogy nem elegendő szakmailag magas színvonalon, megfelelő, de szakkifejezésekkel tarkított (információ 'előadás'), információátadás, hiszen akkor az információbiztonsági szabályzat is működőképes lenne. A Szakmai elváráson túl az adott, kockázatértékelés eredményeképpen meghatározott tudás, alkalmazási gyakorlat, szabály ismeret átvitele mellet legalább ennyire fontos, hogy az információ célba is érjen, szabály megértés, szabály alkalmazás legyen belőle.

Tehát hogyan lehetséges ezt úgy csomagolni, úgy közvetíteni, hogy

- fogyasztható, érdekes legyen, felkeltse az érdeklődést ("igen, ez fontos, releváns számomra, a folyamataimban, vagy magánéletemben")
- kongruens legyen, (vagy beépíthető új információt tartalmazzon)

- meggyőzze az alkalmazás szükségességéről.

Mivel a modell többezres mintán levizsgáltam és mértem, így alkalmazhatóságáról a gyakorlatban is meggyőződtem. Ebből arra következtetek, hogy a modell alkalmazhatósága teljesült.



68. ábra: Az információbiztonsági oktatási modellje, forrás: saját szerkesztés

A 68. számú ábrán az információbiztonsági oktatási modell vizualizációja látható.

A modell jobb megértéséhez és jobb alkalmazhatóságához az alábbiakban röviden kifejtem, hogyan lehetséges a gyakorlatban történő alkalmazása. Ez természetesen munkaszervezetenként eltérő lehet.

- Miért? Ebben a pontban választ kell tudni arra tartja fontosnak a szervezet. Pl.: jogszabályi kötelezettség, milyen kockázatot csökkent, stb. (Ezzel párhuzamosan a ‘célom céljára’ is

választ kell adni, milyen eredményeket várunk el, hogyan kívánjuk az mérni, mikor és hogyan érjük el ezeket az eredményeket)

- Mit? A kockázatértékelés vagy éves terv keretében kitűzött cél, hogy mit oktatunk, mi az amit először és mi az amit később veszünk sorrra, ezek kötődését is érdemes áthondolni. Mi a kulcsüzenet, hogyan mérjük majd, hogy a kulcsüzenet átment-e.
- Hogyan? Hogyan oldjuk meg, hogy a kulcsüzenet(ek) kapcsolódási pontokat találhatnak, a közlés érthető legyen, gyakorlatba átültethető. Milyen tálaljuk, hogyan adja el saját magát, milyen plusz nyújt. Milyen csatornát használunk, az minden résztvevő számára megfelelően hozzáférhető-e.
- Kinek? Szerepkörök azonosítása megtörtént-e, annak megfelelően lett-e minden további paraméter kidolgozva.
- Mikor? A konkrét időpont (szabadság, határidős projektek, stb.) kapcsán érdemes tájékozódni, hogy a teljes ciklus, méréssel együtt kivitelezhető legyen. A résztvevők hogyan tudják a(z aznapi) vagy általában a napi folyamataikba illeszteni.
- Ki? Ki szervezi, ki tartja, ki kommunikálja a képzéssel kapcsolatos teendőket, meghirdetés, vizsga, mérés, általános kérdésekre ki válaszol?.
- Hol? A platform, vagy az adott helyszín bejárása, kipróbálása, szűk körű próba.
- Mérés és visszacsatolás. A legfontosabb, hogy a végén megtudjuk, az egész ciklus milyen eredményeket hozott. Le tudjuk-e mérni, ki tudjuk-e mutatni. Mikor hajtsuk végre a mérést, egy vagy időben eltolva több mérés legyen. Elegendő-e a visszajelzések száma, megkapjuk-e és nyitottak vagyunk-e azokra a visszajelzésekre, amelyek a szabály napi gyakorlatban való alkalmazhatatlanságára, predesztinált szabályszegésre hívja fel a figyelmet. Itt a visszajelzési csatorna biztosítását emelem ki. Azaz az oktatás, tréning során lehetősége van a munkavállalónak tetszőleges munkafolyamatával vagy magánéletbeli kérdést feltenni. Olyat is, amely arra utal, hogy az adott szabály, elvárás nem vagy nehezen alkalmazható a munka folyamatában. Ennek feltárása kulcsfontosságú, mint ahogy disszertációban is megfogalmaztam a nem a kivételekkel van a gond, hanem azzal, ha azt nem szabályozott módon teszi és az egész szabályzatot hagyja figyelmen kívül. Voltaképpen itt nyer értelmet a teljes folyamat, a támogató biztonság, a felhasználók támogatása, a szabálykövetési hajlandóság rutiszerűvé válása.

A modell alkalmazása során tehát javasolt törekedni minden egyes kérdésre kiterjedő válaszadásra még az oktatási ciklus megkezdése előtt.

Az egyes oktatási blokk során alkalmazott, meghatározott kockázatra alkalmazott kockázatcsökkentő intézkedés, előírt szabályzatban meghátorozott előírásra a modell alkalmazásának segítségével vázlatosan kidolgozott blokk. Ezen blokkok nagyságrendileg 12-20 perc között mozognak. Tantermi képzésnél a létszámot javasolt 50 fő alatt maximalizálni, élő (online) képzés esetén pedig a jó kép és hangminőség érdekében maximalizálni.

Az alkalmazott példa gondolati íve:

Jelszóbiztonsági elvárások

Kérdések, ki mit gondol róla, mi van a fejekben, mi a jelenállapoti alaptudás a témában? (A csoportnorma kialakul a visszajelzések alapján).
Közös munka, társasjáték, szedjük össze mit gondolunk a jó jelszóról. (Mi szerepel a szabályzatban, kvíz lehetőség, nyertes hirdetése.)
Érdekességek a témában, visszajelzések és dicséret az elhangzottakra.
A storyline-nal való kapcsolatok (star wars, vagy más elemek, panelek, mondatok).
Tipikus átverések ismertetése, volt-e már hasonló tapasztalat, egyéni, családban ismeretségi körben.
Önként jelentkező felkérése a jelszó begépelésére.
Demo, a jelszó visszafejtése, közben az egyes lépések értelmezése, a show, érdekesség, az élményszerzés.
Közös megbeszélés, a szabályzat elvárásai és annak alkalmazhatósága.
Összefoglalás és tanácsok a magánéleti jelszó használatra is.

Céges bankkártyakezelési biztonsági elvárások

Kérdések, ki mit gondol róla, mi van a fejekben, mi a jelenállapoti alaptudás a témában? (A csoportnorma kialakul a visszajelzések alapján). Mindenkinek van bankkártyája, mit tudunk róla, fogjuk meg vegyünk a kezünkbe.
Szabad szemmel, vizuálisan leolvasható információk és azok kockázata. Mikrokamerák bemutatása. Megoldás, legalább a CVC kód védelme.
Közös munka, társasjáték, szedjük össze mit gondolunk, volt-e már valakinek rossz tapasztalata, visszaéltek-e már a bankkártyájával, vagy a családban, ismeretségi körben.
Érdekességek a témában, visszajelzések és dicséret az elhangzottakra.
A kártya tartalmának kiolvasása, mint kockázat.
Önként jelentkező felkérése a bankkártyájának az átadására.
Bemutató, a bankkártyán található információk kiolvasása, közben az egyes lépések értelmezése, a show, érdekesség, az élményszerzés. Az utolsó 10 tranzakció bemutatása (kizárólag) a kártya tulajdonosának, hogy szóban igazolja vissza, hogy ezeket a tranzakciókat felismeri. Így mindenki előtt hallhatóan elmondja, hogy valóban ezek az ő fizetési tranzakciói.
Közös megbeszélés, a szabályzat elvárásai és annak alkalmazhatósága.
Összefoglalás és tanácsok a magánéleti bankkártya és netbank használatra is.

Ezen oktatási struktúra és módszertan úgy került kialakításra, az eddigi kutatási és oktatási tapasztalatok alapján, hogy az embereket foglalkoztató kérdésekre adjon választ. És az érdeklődést, a megértési és befogadási hajlandóságot megragadva egyrészt a szabályzat erős

állításait, kivonatos formában, a kockázatok bemutatásával alátámasztva kapja meg. Ez, ahogy már kifejtettem, azért rendkívül fontos, mivel így saját belső meggyőződéséből válik szabálykövetővé, a kongruens belső világához tudja igazítani a kapott új ismereteket. Ezeket mivel személyesen megtapasztalta, meggyőződése révén a gyakorlatban is alkalmazni fogja. Idő és kérdések függvényében az előadás közben visszajelzések révén egyéb tipikus elterjed átverési formák és kivédésük bemutatására is sor kerülhet.

Ezen kívül megjelennek még: szórakoztató, látványos elemek, gondolati kötődést támogató szófordulatok és mondatok (pl.: cseréld a jelszavad, mind a fogkefédet 3 havonta; ne oszd meg a kocsikulcsot, mint ahogy a jelszavadat se.) Állításainkat, ha lehetséges támasszuk alá, egy jó mondás, egy jó történet egy rövid demo bemutatása a kockázatok megértése érdekében javasolt. A jobb megjegyezhetőség érdekében törjük át a fogalmi korlátokat, egyéb kapcsolódási pontok, szerepkör alapúan, pl.: vezetőtől a személyes példamutatás is elvárt, adjunk rá példát: szerezz be a kollégádinak információbiztonsági plakátot a munkaterületre. Kössük össze dolgokat, amikor lecsukod a gépet, zárold előtte. Amikor veszed a táskád, zárold a gépet előtte, stb. Kerüljük az szakszavak használatát.

Kérdésekkel operálás lehetősége: amikor a résztvevő mondja ki a választ, így jobban tud azonosulni vele, mintha direkt állításként kapja. Visszakérdezés, figyelem fenntartása, mi jut erről eszébe, milyen saját sztorija van, ossza meg, legyen interaktív az előadás. Önként jelentkező, adjunk lehetőséget a bevonódásra, annak is élmény aki kijön a demóhoz segíteni és annak is aki megéli, hogy nem csak előre felvett klisét kap.

4.2.7. AZ OKTATÁS UTÁNI KÉRDŐÍV KIÉRTÉKELÉSE

A 8. Mennyire tartja aktuálisnak a rendezvény témáját? Miként ítéli meg a rendezvény témájának aktualitását? kérdésre adott válaszok átlaga 9,44 volt.

2. Mennyire érezte hasznosnak az alábbi témaköröket? [SIP célja]	8,2
3. Mennyire érezte hasznosnak az alábbi témaköröket? [Jelszó választás]	9,2
4. Mennyire érezte hasznosnak az alábbi témaköröket? [Telefon használat]	8,16
5. Mennyire érezte hasznosnak az alábbi témaköröket? [Gyerekekkel való bánásmód]	8,6
8. Mennyire tartja aktuálisnak a rendezvény témáját? Miként ítéli meg a rendezvény témájának aktualitását?	9,44
9. Összességében mennyire volt hasznos az Ön számára a rendezvény?	8,84
10. Az oktató értékelése különböző szempontok alapján. [Jól kezeli az időt.]	8,92
11. Az oktató értékelése különböző szempontok alapján. [Új információt ad.]	9,32
12. Az oktató értékelése különböző szempontok alapján. [Érdekes/fenntartja az érdeklődést.]	9,36
13. Az oktató értékelése különböző szempontok alapján. [Ajánlaná-e másnak is a munkaszervezetben a tanfolyamot?]	9,68

14. táblázat: Mennyire tartja aktuálisnak a rendezvény témáját? Miként ítéli meg a rendezvény témájának aktualitását? kérdésre adott válaszok átlaga, forrás saját szerkesztés

Ugyanakkor, bár nem tárgya fő kutatásomnak, de megfigyeléseim alapján az előadó személye, annak megítélése, elfogadása, (szakmai és emberi) elfogadhatósága befolyásolhatja az információ befogadást. A kérdésekre kapott átlagos pontszámokat, válaszokat a 14. számú táblázatban foglaltam össze.

A 8. Mennyire tartja aktuálisnak a rendezvény témáját? Miként ítéli meg a rendezvény témájának aktualitását? kérdésre tehát átlagosan 9,44-es érték született a 10 fokozatú skálán. Amely alátámasztja, hogy a felhasználók nyitottak és érdeklődőek az információbiztonság témakörei és a releváns kockázatok, kivédése, ezen tudás gyakorlatban való alkalmazása iránt.

A 14. Önnek személyes véleménye alapján mi volt ami legjobban tetszett vagy legjobban megragadta a figyelmét? kérdésre lehetőség volt szabadszavas választ adni, mivel a zárt kérdésekkel könnyű felmérni a súlyokat, de új területek, preferenciák és miértek megválaszolására, mégha jóval nehezebb kiértékelni a szógyakoriságot, talán képes többet mutatni.

Elvégezve az ilyenkor már bemutatott műveletsoraz alábbi szófelhőt készítettem, amely azt mutatja, hogy a példák, videók, történetek, a gyakorlatias megközelítés keltette fel leginkább a résztvevők figyelmét és tetszését.

69. ábra: "Önnek személyes véleménye alapján mi volt, ami legjobban tetszett vagy legjobban megragadta a figyelmét?" kérdésre adott szabadszavas válaszok szófelhője, forrás: saját szerkesztés

A kapott szófelhő is alátámasztja, hogy a modellem a gyakorlatban is alkalmazható, a kívánt hatást éri el.

A leggyakoribb 10 szó: peldak, videok, gyakorlatias, tortenetek, jelszo, erdekes, hasznalat, biztonsagos, szemleletes, esetek volt.

A 15. Mennyire valószínű, hogy részt kíván venni a hátralévő két további oktatási modulon? [További modulokon való részvételi szándékom:] kérdésre a válaszadók átlagosan 9,15-ös értéket adtak a 10 fokozatú skálán, tehát arról adtak tanúbizonyságot, hogy a viszonylag drága (munka)idejük ellenére információbiztonsági oktatás annyira felkeltette érdeklődésüket, hogy önkéntesen részt vennének a következőn.

Tehát nem elegendő a szabályzat megfelelő elkészítése és kiadása, hanem annak kommunikációjára, oktatására is erőforrást kell szánni.

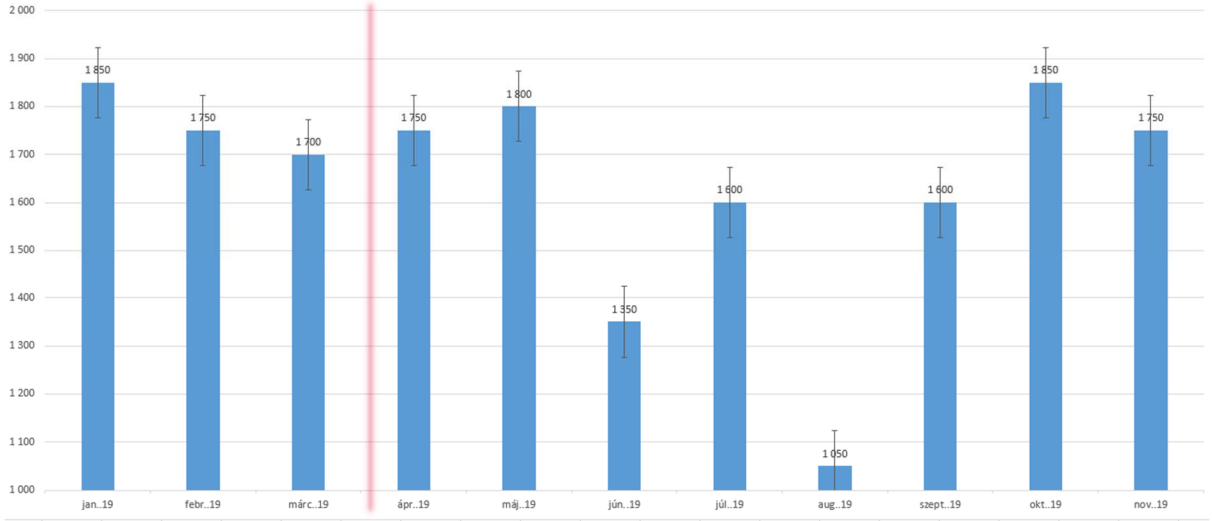
Fontos tehát a hatékonyság megértése az információbiztonsági oktatások szempontjából. Nem elég tudni a szabályokról, hanem mélyen hinni kell bennük, megérteni, hogy az én érdekeimet, a munkáltatóm érdekeit védik és ha nem tartom be, akkor lehet, hogy egy komoly incidenssel akár a munkahely is, annak reputációja is veszélybe kerül.

Hipotézisem alátámasztása érdekében szerencsém volt két külön munkaszervezetnél is vizsgálatot végezni olyan szempontból, hogy kiadásra kerülő IBSZ (Információbiztonsági szabályzat) és IBP (információbiztonsági politika) kihirdetése előtti és utáni trendek vizsgálatára nyílt lehetőségem.

Az információbiztonsági szabályzat 30 oldal alatti terjedelmű, így viszonylag rövidnek mondható. Szerepkör alapú kivonat nem készült hozzá. Az intraneten került publikálásra, és a vezetői körben a köröztetése is megtörtént. Az információbiztonsági politika 3 oldal terjedelmű, az intraneten került publikálásra, és a vezetői körben a köröztetése is megtörtént.
Megfigyeléseimet a felhasználói viselkedés változásra összpontosítottam, azt kívántam vizsgálni, hogyan változik a felhasználói bejelentések száma. Sajnos az intranet oldalon történő szabályzat elolvasási, letöltési, megnyitási statisztika nem állt rendelkezésre. Így arról, hogy pontosan hány munkavállaló nézte meg, vagy olvasta el, nem áll rendelkezésre adat.

4.2.8. "A" VÁLLALATI BEJELENTÉSI ESETSZÁM ELEMZÉSE

Az "A" vállalatnál 2019 januárjától 2019 novemberéig látható idősort ábrázoltam az alábbi diagramon.



70. ábra: A vállalat bejelentési esetszáma az IBSZ megjelenése előtt és után Forrás saját szerkesztés

A 70. számú ábrán piros színnel jelöltem az IBSZ kiadása kapcsán figyelendő időintervallum kezdetét.

Az IBSZ publikációja 2019 áprilisában történt meg. Szignifikáns változás a bejelentések számában nem látható.

71. ábra: képernyőkép az "A" vállalat intranet oldaláról, részlet.

Az 71. ábrán az látható, hogy hibahatáron belül mozog a bejelentések esetszáma, augusztusban a vállalat az alkalmazottak jelentős részét szabadságra küldte a nyári karbantartási munkálatok alatt.

A vállalatnál bevett gyakorlat szerint a szabályzat elhelyezésre került az intranetről is elérhető szabályzat tárba, valamint egyes főigazgatóságok vezetői kaptak egy körlevelet az új szabályzat érvénybe lépéséről. Látható, hogy a szabályzatban egyébként megjelenő bejelentési kötelezettségről feltételezhetően nem értesültek a munkavállalók, vagy annak a szabályalkalmazás gyakorlata legalábbis csorbát szenvedett.

4.2.9. "A" VÁLLALAT MUNKAVÁLALLÓINAK ÉLŐ INFORMÁCIÓBIZTONSÁGI OKTATÁSA

A vizsgasor összeállításakor a kidolgozott módszertant követtem, azaz a tartalmi elemekkel összhangban több kérdés a látványos, szórakoztató elemekre vonatkozott. A kérdések kiválasztása kétféle módon történhet, az oktató választja ki, vagy a rendszer véletlenszerűen választja ki a Moodle rendszerben. Ebben az esetben nem minden kérdés fordul elő a tesztekben, azaz a teszt során bizonyos halmazokból véletlenszerűen generálódnak be a kérdések, azok sorrendje is véletlenszerű.

A teszt neve: Vizsga az interaktív információbiztonsági előadásokhoz

Kurzus neve: Vizsga az interaktív információbiztonsági előadásokhoz

Befejezett és pontozott első próbálkozások száma: 4370

Összes pontozott próbálkozás száma: 7039

Az első próbálkozások átlagos pontszáma: 82,62%

Az összes próbálkozás átlagos pontszáma: 81,73%

Az utolsó próbálkozások átlaga: 89,97%

A legjobb osztályozott próbálkozások átlaga: 90,09%

Median pont: 90%

Szakmai berkekben az az elvárás, hogy az elért pont és elérhető összes pont számai alapján olyan 50-75% között legyen az arány. Itt láthatóan az elért eredmények magasabbak voltak, azaz könnyebb volt a feladatsor, de ez a teszt összeállítása során szándékos döntés volt, hogy egy viszonylag könnyű feladatsor került összeállításra. Annak érdekében, hogy pozitív visszacsatolás, siker élmény legyen az önkéntes vizsga (teszt) elvégzése. Mivel szakmai álláspontom alapján az önkéntes teszt, vagy kérdőív, vagy egyéb általában véve bármilyen ilyen tevékenység szintén hozzájárulhat a biztonságtudatos magatartás és tudás szinten tartásához.

A median jelentése matematikai értelemben a sorba rendezett adatok közül a középső, teszt szempontjából a hallgatók fele érte el azt a pontszámot.

Ami még megállapítható az adatokból, hogy 82,62% -ról 89,97%-ra növekedett az eredmény az újból letehető vizsga eredményeképpen. Azaz mivel a (vizsga) teszt megoldás, annak ismétlési

lehetősége is a modell része, szándékosan úgy került beállításra, hogy a teszt akárhányszor megismételhető legyen és a rendszer mindig a legjobb, legmagasabb elért pontot vegye figyelembe. Így már önmagában ezen eredmények, fejlődés is alátámasztja, hogy oktatással fejleszthető az információbiztonsági tudás szint. Hiszen kimutatható, hogy sokan újra elvégezték a tesztet és jobb eredményeket értek el. (Habár a kellő pontszámot már megszerezték és nem volt kötelező újra elvégezniük).

Median: 100%, ha a próbálkozások legalább fele elérte a 100%-os pontszámot

Szórás: az össz. pontszámok szóródása.

Az adatsorok jellemzéséhez a középértékeken kívül fontos tudni, hogyan helyezkednek el ehhez viszonyítva az adatok. Mindezek érdekében pontszámításhoz tartozó aszimmetria (ferdeség) a normális eloszlású mintához képest aszimmetria esetén a 0 normális, míg ha pozitív, akkor jobbra tolt, felkészült a hallgató vagy könnyű a dolgozat, míg ha negatív vagy balra tolt, akkor gyengék a hallgatók, vagy nehéz a dolgozat, cél -1 és 0 között. A konkrét teszt esetében ennek értéke a pontszámeloszláshoz tartozó aszimmetria (legjobb osztályozott próbálkozás esetén)

-0,993, azaz intervallumon belül található.

Pontszámeloszláshoz tartozó asszimetria: csúcsosság. A pontszámeloszláshoz tartozó csúcsosság, azaz hogyan viszonyul a normál eloszláshoz, amely normál eloszlásnál:0. Ez a görbe két oldalának meredekségére jellemző, ha nagyon meredek a csúcs akkor bizonyos értékek túl gyakran fordulnak elő. A pontszámeloszláshoz tartozó csúcsosság mértéke legjobb osztályozott pontszám esetén 5,15. (Ez a görbe két oldalának meredekségére jellemző, azaz a tesztben bizonyos pont értékek gyakrabban fordulnak elő. Ez egyébként nem csoda, hiszen a jó értékek gyakoriak.)

Belső konzisztencia együtthatója: Cronbach-alfa: a tesztkérdések koherenciájának mértéke. a teszt homogenitisát méri a teszt két felének korrelációjával becsülhető.

hibaarány: a pontszámok szóródásának oka: a különböző próbálkozások pontszámain eltérnek, vagy véletlen lehet az oka. Ezt utóbbinak a mértéke a hiba arány.

Standard hiba: átlagtól való eltérést mutatja.

A tesztszerkezet elemzése a kérdésre vonatkozó statisztika kapcsán az

eszközmutató facilit index használatos, az átlagos pontszám százalékban kifejezve jellemezhető: F-fel, ahol F:

F: < 5 nagyon nehéz vagy rossz a kérdés

6-10 nagyon nehéz

11-20: nehéz

21-34: kicsit nehéz

35-64: átlagos

65-80 elég könnyű

81-89: könnyű

90-94 nagyon könnyű

95-100 kivételesen könnyű.

A teszt kérdések F indexeinek átlaga: 89,24%, amely a tervezett célnak megfelelő érték.

A szórás: standard deviation, a válaszolók válaszainak szórását méri, százalékban kifejezve és ezzel azt is, hogy mennyire diszkriminatív. Mennyire tud különbséget tud különbséget tenni a jó és kevésbé jó tanulók között. A teljes tesztsor egyes kérdéseinek szórásainak átlaga 22,75%. Ez külön egyes kérdésekre is kiszámítható.

A diszkriminációs index: a kérdésre adott pontszám és a teljes pontszám korrelációja, %-ban kifejezve, amely azt méri mennyire különíthetőek el a kérdéssel jobb és gyengén teljesítő válaszadók. A magasabb érték a jobb, az adott kérdés esetén (jobban teljesítők a teszt többi részén is jobban teljesítenek…). A teljes tesztsor egyes kérdéseinek diszkriminációs indexeinek átlaga: 25,79%

A diszkriminációs hatékonyság annak becslése mennyire jó a diszkriminációs index a kérdés nehézséghez képest. A nagyon könnyű vagy nagyon nehéz kérdések nem különböztetik meg a különböző képességű diákokat. A legjobb megkülönböztetést 30-70%os eszközmutató esetén kapjuk. Esetünkben a teljes tesztsor egyes kérdéseinek diszkriminációs hatékonyságainak átlaga: 48,17% amely intervallumon belül van, annak közepén, optimálisnak tekinthető.

Ahogy disszertációmban már célként meghatároztam, nem az információbiztonsági tudás fejlesztése a végső cél, hanem a gyakorlatba való átültetés, olyan módon, hogy döntési szituációban képes legyen azt használni, kongruens módon az alapértékek közé épülve.

A Tudástranszfer célja tehát az alkalmazottak viselkedésének módosítása! A képzés nem a tudatosság növeléséről szól, nem pusztán szórakoztatásról, vagy ismeretek bemutatásáról (átadási kísérletéről) - a tudatosság nagyszerű, de csak akkor, ha viselkedésváltozáshoz vezet.

Rosellini (2020) szerint a tudástranszfer jelenlegi modelljei nem elégségesek azoknak a tényezőknek a meghatározásában, amelyek kezelik az ismeretátadás hatásait a folyamat különböző ciklusaiban, ahol egy munkaszervezet hagyományos képzési programokat alkalmaz. A kutató célja például, hogy azonosítson összefüggéseket a hatékony tudástranszfer és a viselkedési változás között a képzési környezetben. Ezeknek a modelleknek a vizsgálata teáht azzal foglalkozik, hogy a képzés hogyan befolyásolja az ismeretátadást, hogyan befolyásolja a tudás átadása a viselkedés változását és hogyan befolyásolja a viselkedés változása az általános munkateljesítményt.

Éppen ezért fontos volt már a kutatás kezdetén annak megtervezése, hogyan lehetséges majd a szabálykövetés változásának mérése. Azaz egész pontosan nem csak az, hogy egy kérdőívben igen vagy nem választ jelöl meg, ahogy a 2013-as kutatási beszámolóban is céloztam, rá, hogy esetleg csak a vélt vagy valós jó válasznak próbál megfelelni. Hanem sokkal inkább azt szerettem volna feltérképezni, hogy valóban beépül-e a viselkedési mintába, szokásba az oktatást követően.

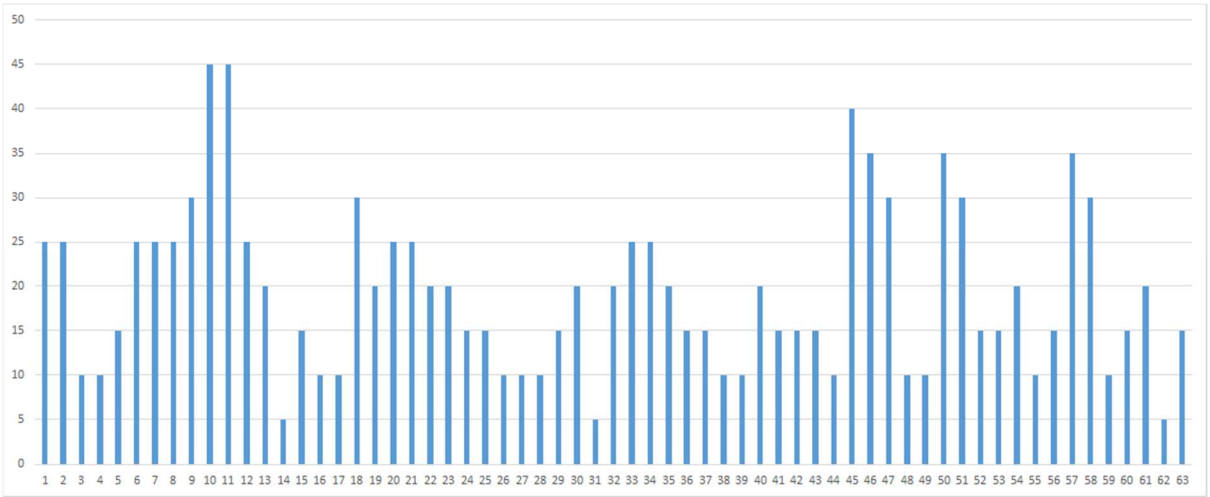
Ennek érdekében a módszertan szerinti kidolgozott oktatásban az egyik kulcsüzenet az volt, hogy "jelentsd be", ha szokatlant tapasztalsz, jelentsd be a spam, kártékonynak tűnő leveleket, kért segítséget, stb. Ennek érdekében havi rendszerességgel nyomon követtem a bejelentési csatornákon tapasztalható esetszámokat.

Ennek eredményeképpen az egyik kulcsüzenet hatékonyságának és gyakorlatba való sikeres átültetésének alátámasztása a bejelentési csatornákon megjelenő esetszám növekedés is alátámasztja.

A bejelentési csatornák és lehetőségek álltak rendelkezésre: e-mailben, ticketing rendszerben és telefonon. Mindezek érdekében az egyes bejelentési csatornák összesített eredményét vizsgáltam. Valamint az oktatásokat megelőző és lezáró intervallumból is figyelembe vettem minimális terjedelműt, hogy a változások jól nyomon követhetőek legyenek.

Az előadás után tapasztalható kérdések

Az előadások során rögzítettem, hogy az egyes oktatások végén, a formális lezárást követően mennyi ideig maradtak még résztvevők kérdezni, egy vagy több személy.

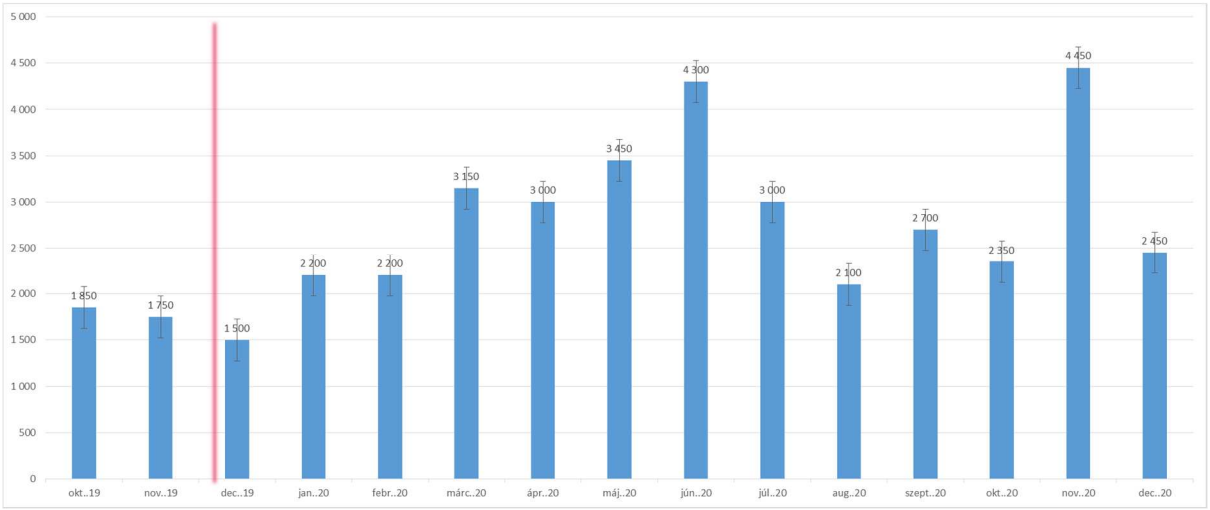


72. ábra: Az élő előadások után feltett kérdések megválaszolására fordított idő, forrás: saját szerkesztés

Átlagosan 19,28 perc volt minden egyes előadás után amikor a témában releváns, részben céges, részben magánéletbeli érdeklődést kielégítő kérdésekre válaszoltam. Ez hozzávetőlegesen kevesebb, mint az előadás terjedelmének ⅕-e. Ennek eloszlását a 72. számú ábrán lehet látni. Megítélésem szerint ez egy rendkívül fontos része az oktatásnak (tréningnek) amikor a visszakérdezésre, jobb megértésre, visszacsatolásra nyílik lehetőség. Azt is komoly eredménynek kell tekinteni oktatások, tréning során, ha a résztvevők aktivizálódnak, aktívak, kérdéseket tesznek fel. Mivel a kérdések feltevés segít abban, hogy a csoport felszabadultan tudjon kérdezni a téma széles spektrumában. Sok, jelentős számú kérdésfeltevés, történetmesélés (storytelling fontosságáról már írtam) azok a többeket izgató, de feltenni nem mert kérdések is előjöhetnek, amelyek aztán a munkafolyamatokban történő alkalmazást pontosan a helyére illeszthetik.

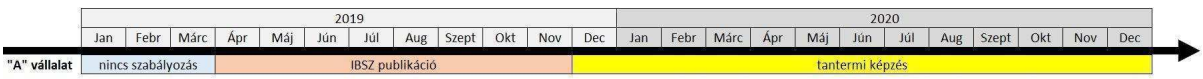
A kiértékelést és változást alátámasztó vizuális bemutatás

Bejelentések száma, havi bontásban:



73. ábra: A vállalat bejelentési esetszáma az elő képzés előtt és után, forrás: saját szerkesztés

Az élő képzések 2019 november utolsó napjaitól (piros vonallal szimbolizálva) 2020 november végéig tartottak. Az ábrán megfigyelhető az augusztusi karbantartási időablak mellett az, hogy szignifikánsan nőttek a bejelentés számok. Valamint 2020 júniusában és novemberében egy-egy jelentősebb incidenst is észleltek a felhasználók.



74. ábra: Az"A" vállalat idősoros nézete, forrás: saját szerkesztés.

Az ábrán jól látható, hogy 2020. januárjában a hibahatáron kívüli növekedés látható. A 2020 augusztusi csökkenés a nyári szabadságolások miatt, betörés látható a diagramon.

Vizuálisan is jól látható, hogy a módszertan szerint megtervezett oktatások következtében nem csak a szabályzat ismerete, de a viselkedés is megváltozott. Amely a gyanús levelek bejelentésében számszerűsíthető eredményt hozott. A valós, megértést és szabálykövető magatartást elváró, azt megkövetelő oktatások hiánya, - ide értve a disszertációmban bemutatott intervallumokat, ahol „csak" szabályzat állt rendelkezésre - rendkívül káros lehet. Ezt a kárt egyrészt a disszertációmban bemutatott soft tényezők bemutatásával is alátámasztható, amelyek hatnak a csoportra (csoportnyomás révén), és hatnak az egyénre, annak viselkedésére, szabályismeretére, szabálymegismerési, szabálykövetési hajlandóságára. Másrészről ezen károk egy-egy incidens elhárítása és felszámolása kapcsán (kiesett) munkaórákban mérhető, így akár forintosítható is. Mivel a munkaszervzeteknek elemi érdeke a hatékony információbiztonsági oktatás, így annak elmaradása, vagy kisebb hatékonysággal való megvalósítása kárt okozhat.

4.2.10. AZ I. NEMZETI KIBERVERSENY TAPASZTALATAI

Az I. Nemzeti Kiberversenyen induló Nemzeti Közszolgálati Egyetem Rendészettudományi Kar csapata kért fel felkészítőnek 2016 év végén. Így lehetőségem volt az általam kidolgozott modellt alkalmazni ezen csapat felkészítése során is. A jelenléti oktatás szabályalkalmazási gyakorlatának alkalmazhatóságára és hatékonyságára kiváló példa a Nemzeti Kiberversenyen elért eredmény. A 2017 februárjában került megrendezésre az I. Nemzeti Kiberversenyen. A versenyen az NKE Rendészettudományi Kar által indított csapat is nevezett. A versenyzők felkészítésére a verseny előtt mindössze 2 hónappal kértek fel. Így rendkívül szűk időintervallum állt rendelkezésre. A versenyen 26 jelentkező csapat közül, sikerült a döntőbe jutnia az általam felkészített 4 fős NKE Rendészettudományi Kar csapatának. A verseny alapvető feltevése az volt, hogy Magyarországi és EU-s szinten egészségügyi intézményeket ér kibertámadás. A verseny utolsó fordulójában 4. helyezést ért el a csapat. A rendelkezésre álló nagyon rövid időben a modellem alkalmazásával gyakorlat alkalmazást támogató felkészítést alkalmaztam. Így ezen rövid idő alatt is, az egyébként természetesen rendkívül jó képességű rendészettudományi kar hallgatói országos szinten kimagasló eredményt tudtak elérni.

4.2.11. STATISZTIKAIÖSSZEFÜGGÉS-ELEMZÉS

A statisztikai összefüggés elemzés megkezdése előtt összefüggéseiben és környezetükben is vizsgáltam a rendelkezésre álló adatokat. Ezek egy része csak informális adat, azaz számszerűen nem osztható meg, túlmutat a kutatás területi határain. A számszerű és kvantifikálható adatokon

túl fontosnak tartom megemlíteni, hogy az intranet oldal látogatottsága tekintetében a vizsgált intervallumban a top 250-es listában egész évben 1 szabályzat sem volt havi bontásban vizsgálva. A 250. elem látogatottsága nagyságrendileg 2150 volt. Jellemzően olyan elemek voltak a lista tetején, amelyek nem szigorúan a munkaszervezethez, az elvégzett feladatokhoz, munkafolyamatokhoz kapcsolódnak. Például, de nem kizárólag: étlap, étterem nyitva tartása, üdülési lehetőségek, apróhirdetések, stb.

Mivel a B vállalathoz tartozó tantermi képzést követő bejelentési adatok eloszlása nem tekinthető normálisnak (Kolmogorov-Smirnov próba: t=0.299, p=0.011), ezért a kétmintás t-próba helyett az F próba mellett döntöttem. (6-11. számú melléklet)

ANOVA

Company		Sum of Squares	df	Mean Square	F	Sig.
A	Between Groups	8555750,260	2	4277875,130	9,617	0,001
	Within Groups	9340874,779	21	444803,561		
	Total	17896625,038	23			

15. táblázat: A bejelentések kétmintás t-próba táblázata, forrás: saját szerkesztés

Az A vállalat esetében a varianciaanalízis jelentős eredménye (F=9.617, p=0.001) folytatásaként elvégzett Dunett T3 post hoc próba igazolja, hogy a tantermi képzést követően a bejelentések száma jelentős mértékben növekedett mind az IBSZ publikációt követő szakaszhoz, mind a szabályozás előtti szakaszhoz képest. A szabályozás nélküli, a információbiztonsági szabályzat (IBSZ) kiadását megelőző és az IBSZ publikációt követő, de képzést megelőző szakaszok között nincs jelentős eltérés a bejelentések számában. (6-11. számú melléklet)

Az B vállalat esetében nincs jelentős eltérés a (F=1.126, p=0.303) az IBSZ publikáció és az e-learning képzés között a bejelentések számában. A szabályozás nélküli szakaszhoz képes nem vizsgálható az eltérés, mert nincs elegendő adat. (6-11. számú melléklet)

Mindezek alapján hipotézisem alátámasztását megalapozottnak találtam és **elfogadom**.

4.3. A HARMADIK HIPOTÉZIS VIZSGÁLATA

H3: Az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető.

Az e-learning tananyag és a környezet kialakítása során is maximálisan törekedtem arra, hogy a kidolgozott modellem lehető legtöbb része érvényesítésre, beépítésre kerüljön, természetesen ahol

ez lehetséges volt. Így az alábbiakban röviden bemutatom, hogy milyen megfontolások és beállítások mellett lett a kutatás lefuttatva.

Az e-learning oktatások, összesen három darab e-mail biztonság, jelszó biztonság és adathalász támadások kivédése témakörökben készültek el.

Speciális e-learning szerkesztő eszközzel készült, amely interoperábilis, valamelyest interaktív, akár elágazásokat tartalmazó, nem csak statikus tartalmak megjelenítése képes.

Az e-learning megoldás során az SCORM csomagba importálható, így tetszőleges LMS rendszerben lejátszható. Én a moodle rendszert alkalmaztam, mivel az adott vállalatnál az állt rendelkezésre. A SCORM, Sharable Content Object Reference Model, egy de fakto szabványként tekinthető. https://regi.tankonyvtar.hu/hu/tartalom/tamop412A/2011-0103_10_elektronikus_oktatasi_kornyezetek/ch04s03.html) Az LMS (Learning Management System) tekintetében a moodle rendszer került alkalmazásra.

Az e-learning kurzusok intranet hírként, nem kötelező tananyagként kerültek meghirdetésre. (Pont úgy, ahogy a szabályzatok publikációja). Az e-learning oktatás értelmezésemben és az általam alkalmazott kutatáson belül azt jelentette, hogy kifejezetten e-learning szerkesztő eszközzel készült, elágazásokat tartalmazott. A fejlesztés során arra helyeztem a hangsúlyt, hogy az alapvetően nem élőszereplős előadáshoz képest, a modellem egyes részeit ahol csak lehetett alkalmazzam, a lehetőségekhez képest minél interaktívabb legyen, a színek, formák, példák mind illeszkedjenek az adott tartalomhoz. Ahol lehetséges volt a figyelem további fókuszálása érdekében színezést, kiemelést alkalmaztam. Jellemzően minden képernyőnyi felületen valamilyen további interakció volt elvárt, nem lehetett “csak” olvasással tovább haladni. Grafikai, színvilág, piktogramok, ikonok tartalomhoz történő igazítása, valamint az érdeklődés fenntartása érdekében grafikai megjelenés tervezése is szempont volt. Ugyanakkor egy kibertámadás során felismerhető, felismerendő, tipizálható elemekre a figyelem, fókusz irányítása is megvalósuljon. Mozgással, színezéssel, kiemeléssel, ismétléssel, vagy egyéb módon.

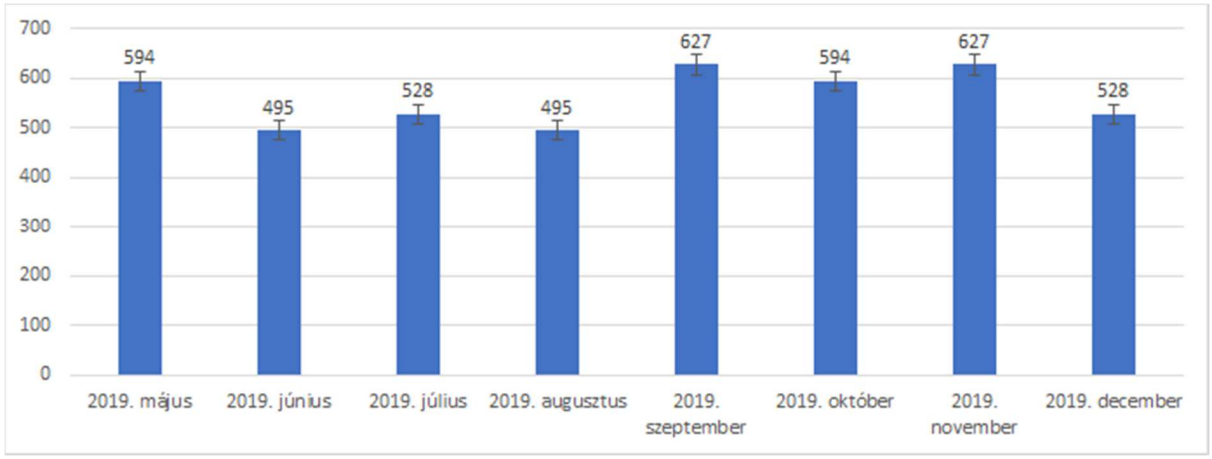
Az e-learning tananyagoknál akárhányszor meg lehetett próbálni megoldani, a tesztek eredményét javítani. A kérdések és válaszok visszanézhetőek voltak. Minden teszt egyes kérdés utána a rendszer visszajelzést adott, hogy jó vagy rossz volt a válasz és miért.

Az e-learning és teszt kérdéseken kívül, de a mellett elhelyezésre került egy visszajelzési lehetőség, amivel értékelni lehetett az e-learning tananyagot és visszajelzést lehetett adni. Ezt külön lehetett, kellett elindítani amennyiben valaki visszajelzést szeretett volna adni, nem volt kötelező és az indításhoz is további interakció volt szükséges.

A ‘“B”vállalatnál 2019 júniusában jelent meg az információbiztonsági szabályzat

75. ábra: képernyőkép az intranet oldalról,:

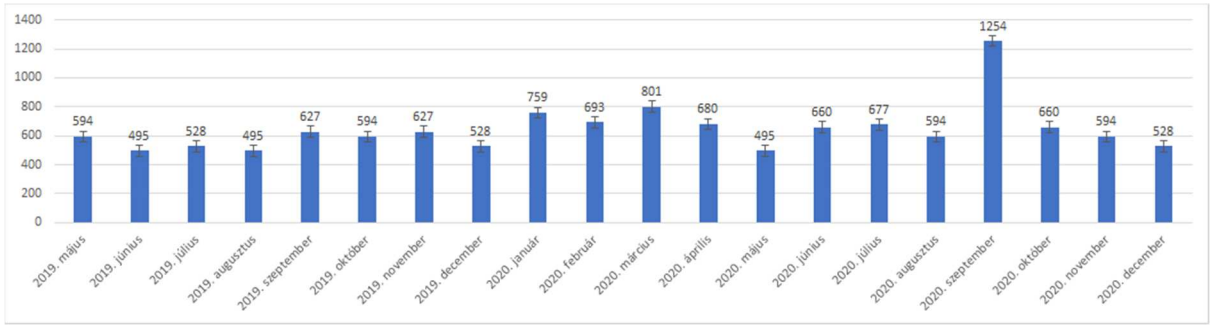
A szabályzat előtti egy hónap és a szabályzat utáni időintervallumban álltak rendelkezésre a bejelentés számok.



76. ábra: A "B" vállalat bejelentési esetszáma az IBP megjelenése előtt és után, forrás saját szerkesztés

Nem látható szignifikáns változás.

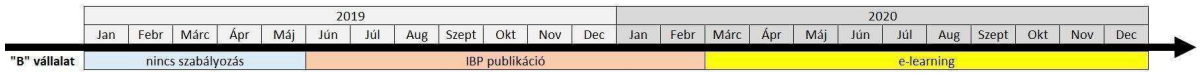
Ezt követően kiadásra kerültek az e-learning anyagok. 2020. márciusban és 2020 júniusban.



77. ábra: A "B" vállalat bejelentési esetszáma az e-Learning oktatási anyagok hatására, forrás: saját szerkesztés

Márciusban némileg magasabb, de hibahatáron belüli a növekedés szám. A júniusi e-learning kapcsán nem észlelhető jelentős növekedés, de a nyári szabadságolások miatt akár a stagnálás is annak tekinthető.

Ami talán még érdekes, hogy a szeptemberben tapasztalt incidensnél azonban a munkavállalók jól vizsgáztak, nagy számban jelentették az esetet.



78. ábra: A "B" vállalat IBP megjelenésének, s e-learning képzésének időintervallumai, forrás: saját szerkesztés

4.3.1. E-MAIL BIZTONSÁG E-LEARNING TANANYAG TESZT KIÉRTÉKELÉSE

Az "E-mail biztonsági alapok" című e-learning tananyaghoz tartozó tesztet 2196 egyedi kitöltő kezdte el megoldani, 2853 darab próbálkozás történt.

A teszt 2019 december 11-étől nyitva van, az utolsó kitöltő 2021.03.08-án volt. A vizsga nem volt kötelező, a felhívást a vállalat intranet oldalán került közzétéve az egyéb közérdekű hír között. Az e-mail biztonság tananyag kialakítása során arra helyeztük a hangsúlyt, hogy az alapvetően nem élőszereplős előadáshoz képest, a lehetőségekhez képest minél interaktívabb legyen. Ennek érdekében kifejezetten tananyagszerkesztő szakprogrammal került megtervezésre és létrehozásra.

A információbiztonsági folyamatok nem kerültek még kialakításra, a felhasználói tudatosság a SANS besorolás szerinti 1. szinten állapítható meg.

A 2853 kitöltési próbálkozás 2196 egyedi személyhez tartozott. Azaz 656 darab második, vagy többedik próbálkozás is volt a teszt kitöltésére, sikeres, vagy magasabb pontszám elérésére. minden számot kicsit kerekíteni?

541 fő kétszer próbálkozott,

91 fő háromszor próbálkozott,

21 fő négyszer próbálkozott,

5 fő ötször próbálkozott,

1-1 fő hatszor ill. hétszer próbálkozott.

A sikeres teszthez 80%-os eredményt kellett elérni. A teszt tetszés szerinti számban megismételhető volt. Első próbálkozásra sikeres vizsgát tett 1781 fő.Első próbálkozásra 415 főnek nem sikerült. Ebből 273 főnek 0 pontja lett. (Itt a session (munkamenet) időtartamokból arra lehet következtetni, hogy valami megzavarta a kitöltés közben, azt vagy hamar becsukta, vagy extrém sokáig tartotta nyitva.

4.3.1.1 E-mail biztonság e-learning tananyagra kapott felhasználói visszajelzések

Az adatok tisztítása után 1008 darab egyedi felhasználó töltötte ki a kérdőívet.

Értékelje egytől ötig terjedő skálán, hogy milyen hasznos volt Ön számára a tanfolyam. (1=nem hasznos, 5=nagyon hasznos)

948-an válaszoltak, átlaga 4,47, amely kimagaslóan jó eredmény véleményem szerint.

Összesen 962 fő adott az előre definiált mezők segítségével visszajelzést:

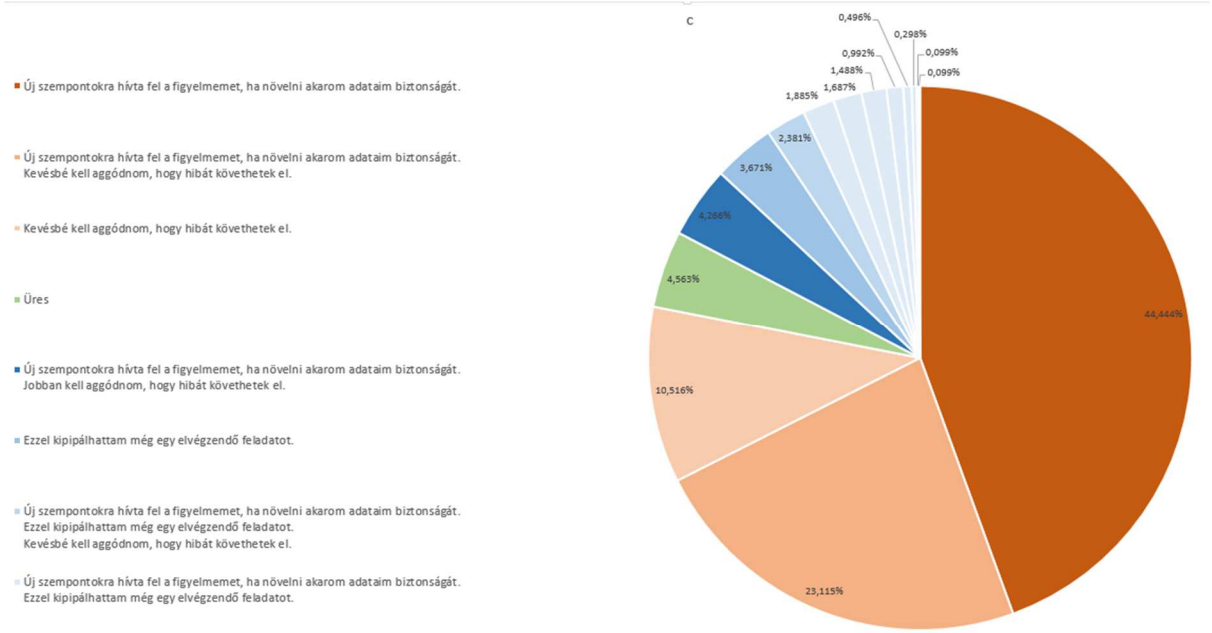
Az e-learniget követően a vizsgázóknak lehetőségük volt visszajelzést adni, amely nem volt kötelező.

Az alábbi előre definiált válaszok mellett szabadszavas válaszokat is meg lehetett adni egy külön mezőben.

Kérjük jelölje be amennyiben hasznosnak találta a tanfolyamot, hogy miért? kérdésre lehetséges válaszok:

- Üres: amennyiben semmit nem jelölt be egyiket sem
- Új szempontokra hívta fel a figyelmemet, ha növelni akarom adataim biztonságát.
- Kevésbé kell aggódnom, hogy hibát követhetek el.
- Jobban kell aggódnom, hogy hibát követhetek el."
- Ezzel kipipálhattam még egy elvégzendő feladatot.

vagy ezek tetszőleges kombinációja.



79. ábra: A tanfolyam hasznosságának felhasználói értékelése, forrás: saját szerkesztés

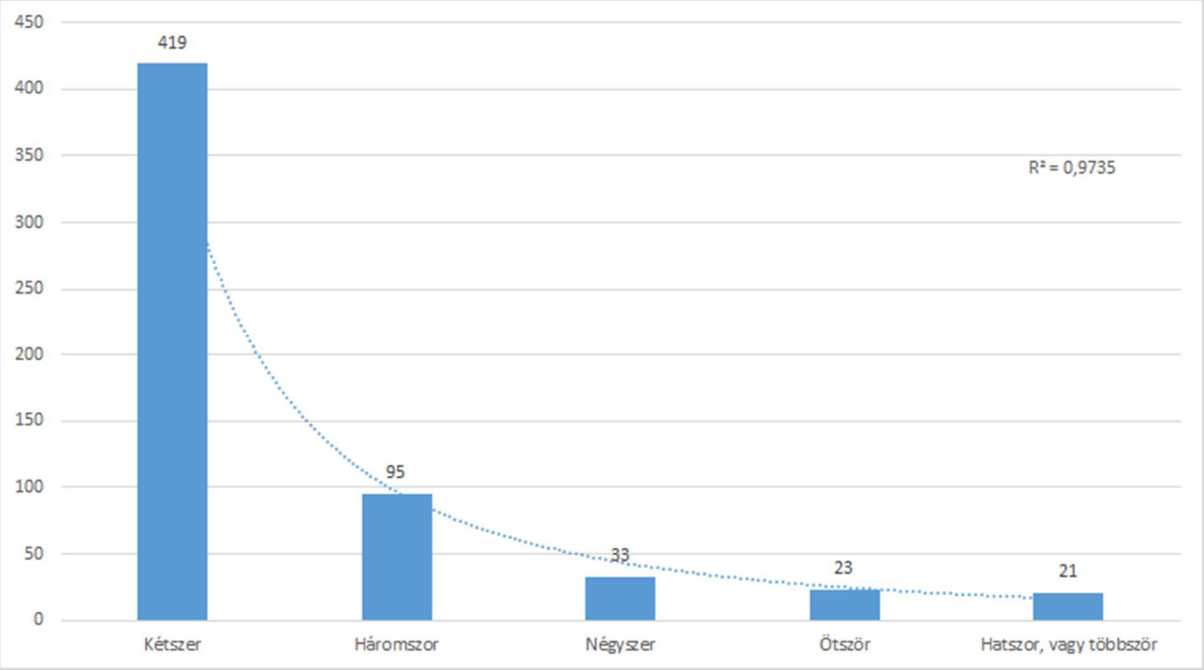
A 79. számú ábráról leolvasható, hogy a válaszadók 78,075%-a jelölte meg az “Új szempontokra hívta fel a figyelmemet, ha növelni akarom adataim biztonságát.” lehetőséget,

A piros és árnyalatai a pozitív visszacsatolást, a zöld a nem adott választ, a kék és árnyalatai pedig a kötelező feladat letudására adnak vizuális reprezentációt.

148-an pedig egyedi szöveges választ is adtak, amely jól jelzi a tananyagra adott aktív részvételi visszajelzést: 15% nagyságrendileg.

4.3.2 JELSZÓBIZTONSÁGI ALAPOK E-LEARNING TANANYAG TESZT KIÉRTÉKELÉSE

Az "Jelszó biztonság kezdő szinten" című e-learning tananyaghoz tartozó tesztet 1976 egyedi kitöltő kezdte el megoldani, 2902 darab próbálkozás történt.
A teszt 2020. április 10-étől nyitva van, az utolsó kitöltő 2021.03.08-án volt. A vizsga nem volt kötelező, a felhívást a vállalat intranet oldalán került közzétéve az egyéb közérdekű hír között. Az jelszó biztonság tananyag kialakítása során arra helyeztük a hangsúlyt, hogy az alapvetően nem élőszereplős előadáshoz képest, a lehetőségekhez képest minél interaktívabb legyen. Ennek érdekében kifejezetten tananyagszerkesztő szakprogrammal került megtervezésre és létrehozásra.
A információbiztonsági folyamatok nem kerültek még kialakításra, a felhasználói tudatosság a SANS besorolás szerinti 1. szinten állapítható meg.
A 2902 kitöltési próbálkozás 1976 egyedi személyhez tartozott. Azaz 389 darab második, vagy többedik próbálkozás is volt a teszt kitöltésére, sikeres, vagy magasabb pontszám elérésére.
664 fő kétszer próbálkozott,
184 fő háromszor próbálkozott,
51 fő négyszer próbálkozott,
12 fő ötször próbálkozott,
15 fő hatszor vagy többször próbálkozott.



80. ábra: Jelszóbiztonság e-learnig tananyaghoz kapcsolód vizsga próbálkozások, forrás: saját szerkesztés

A 80. számú ábrán feltüntettem a trendvonalat, amely hatványos, valamint az r-négyzet értékét, ahol r-négyzet érték felfogható az x varianciájának az y varianciájára gyakorolt hatásaként. A trendvonal akkor a legmegbízhatóbb, ha r-négyzet értéke közel 1. A vízszintes tengelyen az adott számú vizsga próbálkozások kerültek feltüntetésre, míg függőleges tengelyen az ahhoz a próbálkozási számhoz tartozó felhasználók száma. Rá kívánok világítani, hogy önként a felhasználók jelentős száma, többen a sikeres vizsgát követően, csak a maximális elérése érdekében (vagy egyéb okból) újra és újra letették a vizsgát.

A sikeres teszthez 75%-os eredményt kellett elérni. A teszt tetszés szerinti számban megismételhető volt. Első próbálkozásra sikeres vizsgát tett 1587 fő.Első próbálkozásra 216 főnek nem sikerült. Ebből 173 főnek 0 pontja lett. (Itt a session (munkamenet) időtartamokból arra lehet következtetni, hogy valami megzavarta a kitöltés közben, azt vagy hamar becsukta, vagy extrém sokáig tartotta nyitva.

A modell alapján kidolgozott kérdéssor egyik eredménye, hogy ahogy a számokból is látható, a (nagyszámú) próbálkozások döntő százaléka nem az elégtelen pontok növelése érdekében történt, hanem bár elsőre is sikerült a teszt, azaz elérte a válaszadó a szükséges pontszámot, de növelni kívánta azt, vagy kíváncsi volt a kérdésekre. Mivel egyértelműen kommunikálva volt, hogy a kérdések véletlenszerűen kerülnek be a kérdésbankból, így második, vagy újbóli nekifutásra további érdekes kérdéseket kaphatott. A minta kézi elemzése során számos hasonló tendencia volt tapasztalható. Az adatsor önmagáért beszél, jól látható, hogy bár elsőre is

sikeres, a teljesítéshez elegendő volt a pontszám, de a kérdések érdekességéért, vagy a tananyag érdekessége miatt, más indíttatásból újból és újból megoldotta azt a válaszadó.

kalm
7
7,2
7,4
7,83
8
8,5
8,67
9
9,2
9,3
9,5
10

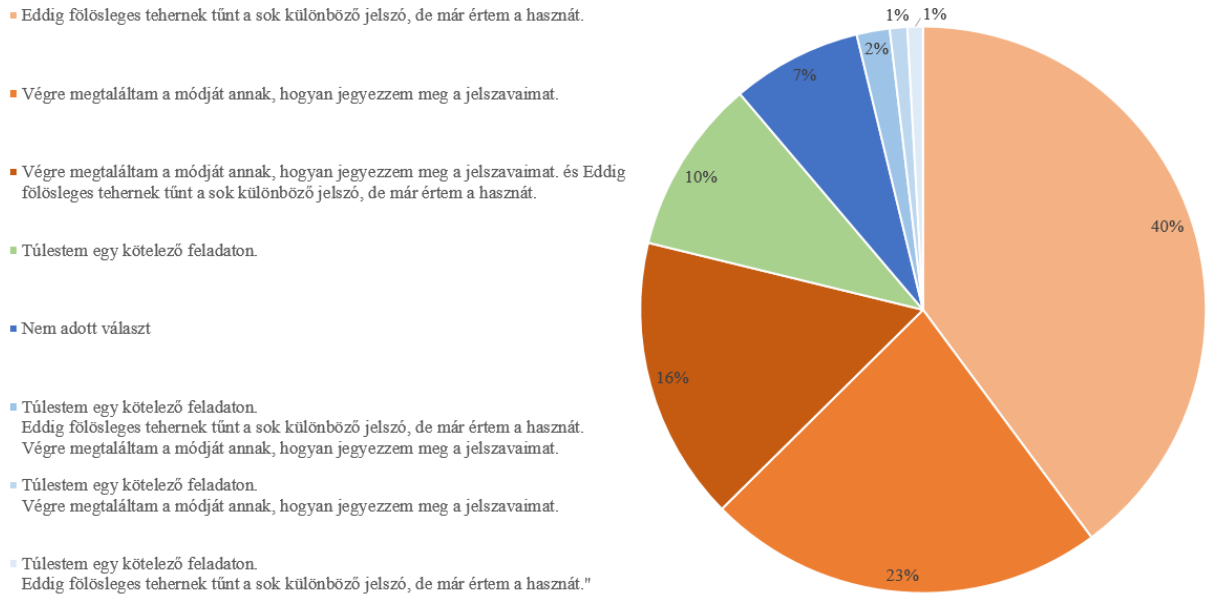
81. ábra: Újból és újból megoldásra ösztönzött munkavállalók a mintában, forrás: saját szerkesztés

A fenti 81 számú ábrán az látható, hogy az adott példaként kiválasztott munkavállaló az adott vizsga tesztet a lehetséges időintervallumban többször, összesen 12-szer oldotta meg, egyre jobb és jobb pontszámokat elérve. Ezáltal fejlődhetett a tudása, mivel a jó kérdésekre, akár tippelgetéssel, vagy más módon de rájött a gyakorlat végére.

Ugyanezen felhasználó másik vizsga moduljában vett tanulási viselkedését vizsgálva hasonló motívum látható: ott is egy folyamatosan növekvő pontszám és összesen 15 darab próbálkozás volt látható, amíg a maximális pontszámot el nem érte.

4.3.2.1. Jelszóbiztonsági alapok e-learning tananyagra kapott felhasználói visszajelzések

A visszajelzéseket megtisztítva, 901 egyedi válaszadó töltötte ki a visszajelzések kérdőívet.
Értékelje egytől ötig terjedő skálán, hogy mennyire volt hasznos az Ön számára a tanfolyam! (1=nem volt hasznos, 5=nagyon hasznos volt)
A válaszadók közül 867 fő adott számszerű értékelés: Ennek átlaga: 4,497
Ebből arra következtetek, hogy a modell alkalmazása teljesült, azaz érdekes és fogyasztható köntösben kaptak szakmai tartalmat. Megvalósult a szakmai tartalom átadására vonatkozó elvárás és az átadáshoz szükséges átviteli közeget, csomagolást is sikerült megfelelően kidolgozni.



82. ábra: "Miért volt Ön számára hasznos a tanfolyam?" kérdésre adott válaszok, forrás: saját szerkesztés

834 válaszadó választott az előre definiált lehetőségek közül. Az ábráról leolvasható, hogy a válaszadók 78,80%-a jelölte meg az "Új szempontokra hívta fel a figyelmemet, ha növelni akarom adataim biztonságát." lehetőséget,

A piros és árnyalatai a pozitív visszacsatolást, a zöld a nem adott választ, a kék és árnyalatai pedig a kötelező feladat letudására adnak vizuális reprezentációt.

4.3.3. ADATHALÁSZ TÁMADÁSOK ELLENI VÉDEKEZÉS LEHETŐSÉGEI E-LEARNING TANANYAG TESZT KIÉRTÉKELÉSE

Az "Adathalász támadások elleni védekezés lehetőségei" című e-learning tananyaghoz tartozó tesztet 2667 egyedi kitöltő kezdte el megoldani, 3454 darab próbálkozás történt.

A teszt 2020. augusztus 10-étől nyitva van, az utolsó kitöltő 2021.03.09-án volt. A vizsga nem volt kötelező, a felhívást a vállalat intranet oldalán került közzétéve az egyéb közérdekű hír között.

Az adathalász támadások felismerését célzó tananyag kialakítása során arra helyeztük a hangsúlyt, hogy az alapvetően nem élőszereplős előadáshoz képest, a lehetőségekhez képest minél interaktívabb legyen. Ennek érdekében kifejezetten tananyagszerkesztő szakprogrammal került megtervezésre és létrehozásra.

A információbiztonsági folyamatok nem kerültek még kialakításra, a felhasználói tudatosság a SANS besorolás szerinti 1. szinten állapítható meg.

A 3454 kitöltési próbálkozás 2667 egyedi személyhez tartozott. Azaz 787 darab második, vagy többedik próbálkozás is volt a teszt kitöltésére, sikeres, vagy magasabb pontszám elérésére érdekében.

419 fő kétszer próbálkozott,

95 fő háromszor próbálkozott,

33 fő négyszer próbálkozott,

23 fő ötször próbálkozott,

21 fő hatszor vagy többször próbálkozott.

A sikeres teszthez 70%-os eredményt kellett elérni. A teszt tetszés szerinti számban megismételhető volt.

Ezt követően statisztikai próbákat végeztem. Vizsgáltam az információbiztonsági szabályzat kiadása előtti, utáni és az e-learning publikáció előtti és utáni időszakokat a felhasználói bejelentések számával vett összefüggést.

6-11. számú melléklet, (One-Sample Kolmogorov-Smirnov Test)

A statisztikai próbák alapján nem volt kimutatható jelentős eltérés a (F=1.126, p=0.303) a szabályzat publikáció és az e-learning képzés között a bejelentések számában. A szabályozás nélküli szakaszhoz képes nem vizsgálható az eltérés, mert nincs elegendő adat.

Oneway

Descriptives

Company		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound	Minimum	Maximum
B	IBSZ publikáció	9	594,00	91,868	30,623	523,38	664,62	495	759
	e-learning	10	676,60	216,133	68,347	521,99	831,21	495	1254
	Total	19	637,47	170,009	39,003	555,53	719,42	495	1254

16. táblázat: A varianciaanalízis leíró statisztikái, forrás: saját szerkesztés

Bár statisztikai próbákkal nem volt kimutatható korreláció ugyanakkor hangsúlyoznám, hogy miért is kiemelkedő jelentőségű ezen megfigyelésem. Míg a teljes szabályzattár megnyitása átlagosan havi 465 darab (a teljes szabályzatára vonatkozó) megnyitással szemben itt a több ezres megtekintés mellett ezres nagyságrendű önkéntes tanulás, majd önkéntes feladatmegoldás és mindezeken kívül ezres léptékben visszajelzés volt mérhető.

4.3.4. E-LEARNING OKTATÁSOK SZÁMADAT KIÉRTÉKELÉSEK ÖSSZEGZÉSE

Mind az e-mail biztonság, mind a jelszó biztonság, mind az adathalász támadások kivédése e-learning esetében elmondható, hogy a nem kötelező, intraneten publikált, de a modell szempontjai figyelembe véve jelentős érdeklődést és aktivitást mutattak a felhasználók.

Az e-mail biztonság, mind a jelszó biztonság kapcsán a szintén önkéntes visszajelzést is nagy számban töltötték ki. A kurzusok számszerű értékelése 4,48 közel maximálisra értékelték. Ezeket a számadatokat úgy értékelem, hogy a modell működőképes nem csak élő, tantermi képzésnél, hanem learning, illetve az intranetes, írott kommunikáció kapcsán, annak segítségével sikerült a felhasználókat elérni, aktivitásra buzdítani és részvételt elérni.

Az egyes, 3 darab e-learning képzés egyedi résztvevőinek vizsgálata során megállapítottam, hogy összesen 3151 munkavállaló vett részt, kezdte el legalább az egyik e-learning képzést.

- jelszó biztonsági e-learning: egyedi felhasználók száma: 1977 (próbálkozások száma: 2902, visszajelzések száma: 901, számszerű értékelést tett: 867, előre definiált szövegszerű értékelést választott: 834, egyedi szöveges értékelést adott: 134 fő.)
- adathalász támadások kivédése e-learning: egyedi felhasználók száma: 2668 (próbálkozások száma: 3454, ehhez a modulhoz nem készült visszajelzési lehetőség).
- e-mail biztonsági alapok e-learning: egyedi felhasználók száma: 2197 (próbálkozások száma: 2853,visszajelzések száma:1008, számszerű értékelést tett: 948, előre definiált szövegszerű értékelést választott: 962, egyedi szöveges értékelést adott: 148 fő)

A zárójelben az összes próbálkozás és további számszerű értékek láthatóak, előtte feltüntetve az egyedi kitöltők számát.
Ezt összevetve az élő előadások után következő kérdezési lehetőséggel az látható, hogy a 90 perces előadás után átlagosan 20 perces további kérdés blokkot igénybe vett a résztvevők egy része. Ahhoz képest, hogy nem volt kötelező, nagy létszámban végezték el a képzést a munkavállalók, valamint nagy létszámban töltötték ki önkéntesen a visszajelzést modult.

Ahogy azt már disszertációmban tisztáztam a tudatosság egy speciálisan magas szintje a a szabályalkalmazás képessége. Így tézisemben azt vizsgálom, a nem kötelezően az intraneten meghirdetett e-learning képzések megtekintése, elvégzése, önkéntes levizsgázás és önkéntes visszajelzés, értékelés megtekintés száma és a szintén az intraneten közzétett információbiztonsági szabályzat megtekintései idősorosan hogyan változtak és egymáshoz képest hogyan változtak.

Összegezve tehát **megállapítottam, hogy az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető, ugyanakkor ez statisztikailag nem kimutatható szignifikánsan, azaz a H3 hipotézisemet elvetettem.** Ugyanakkor kiemelkedő jelentőségűnek tartom, hogy a modellem alapján megtervezett és kivitelezett, javaslataim alapján (nem kötelezőnek, hanem érdekesnek, magánéleti vetületben is alkalmazhatónak kommunikált) oktatási témákat (3 db) publikálva, azon nagy volumenben vettek részt a munkavállalók, oldották

meg önkéntesen. Az e-learning tananyagokkal elért felhasználók és kattintások száma nagyságrendileg magasabb volt, mint a szintén intraneten publikált szabályzatra történő kattintások száma. Ez pedig nem csak az e-learning oktatás elvégzésére, de az e-learning utáni vizsga részre és az azt követő viszajelzés adási részre is igaz. Esetleges további mérésekkel és vizsgálatokra érdemes annak vizsgálata, hogy milyen jelentősége van, hogy az itt óvatosan bevezetett szakszavakra történő további építkezésnek. Milyen módon gyorsítja, támogatja, teszi jobban befogadhatóvá a szabályalkalmazási gyakorlat további fázisait és ezt hogyan, milyen indikátorokkal lehetséges mérni, számszerűsíteni. Így lehetséges annak további vizsgálata, hogy más, vagy milyen indikátort szükséges választani, vagy egyéb kérdőíves felmérést végezni a jövőben.

4.4. NEMMEGFELELŐSÉGI GYAKORLATBÓL FAKADÓ KOCKÁZAT KEZELÉSE

Disszertációmban bemutattam, hogy a szervezeti felsővezetés hatékonyságához szükséges az informatikai rendszerek és információbiztonsági hatékony támogatás is. Számos irányítási rendszer más és másféleképpen közelíti meg a területet. Muha, Szádeczky (2014) Irányítási rendszerek könyvében az IBIR (információbiztonsági irányítási rendszerek kapcsán az ISO 27001 terminológiát követve kiemeli a "képzési és tudatossági oktatások" fontossága mellett a "A képzések hatásosságának mérése"-t is. A "Mérések szükségessége"-t követően a "helyesbítő tevékenységek" közé sorolja a nemmegfelelőségek kezelését. Ezt követően lehetnek megelőző és helyesbítő tevékenységek (Muha, Szádeczky, 2014). Az IBIR (információbiztonsági irányítási rendszer) elvárja, hogy a folyamatokat folyamatosan fejlessze a szervezet. Továbbá elvárja a dokumentált információ fenntartását, "Fontos a dokumentációk megléte, tekintettel arra, hogy a szervezet így tudja bizonyítani a vizsgálatot folytató felé, hogy az IBIR rendszerét a változó környezet és a felmerülő nemmegfelelőségek érdekében folyamatosan fejleszti, törekszik az optimális állapot eléréséért." Muha, Szádeczky (2014). A nemmegfelelőség kezelése kapcsán megelőző és helyesbítő tevékenység jelenik meg, mint lehetőség. Ugyanakkor a szakirodalmi áttekintés során nem találtam olyan megoldást amely arra kínálna megoldást, hogyan lehetséges a nemmegfelelőség növekedése, vagy az általam "compliance distance" növekedése. Ennek lényege, hogy az egyébként mért terület mérési szokása miatt nem megfelelő adatokat szolgáltat, nem sikerült feltárni a nemmegfelőséget. Vagy nem kerül olyan mérés kialakításra, amely ezt a nemmegfelelőséget feltárná. Ennek egyik lehetséges oka, ahogy Babbie (2001) könyvében

szerepel, hogy “észre kell vennünk azonban, hogy egy mérőeszköz sűrűn használt volta önmagában nem biztosíték a megbízhatóságra.” Ugyanannak a mérésnek, vizsgálatnak a megismétlése tehát adhat pontatlan, hibás eredményt, amely így nem alkalmas az eredeti cél a kockázatok változásának érzékelésére. Sadiq et al. (2008) a preventív, detektív, korrektív lehetőségek közül a megfelelőség elérését célzó fenntartható megközelítésnek alapvetően a megelőzésre kell összpontosítania. Ugyanakkor azt is megfogalmazza Sadiq et al. (2007), hogy mind a folyamatok tulajdonosainak, (stakeholders) mind pedig a biztonsági (compliance) felelősnek tisztában kell lennie a folyamattal. Valamint ezen kívül a formális logika nyelvét használja Sadiq et al. (2008), amiből nem csak az következik, hogy szükséges megérteni a compliance officer-nek az adott folyamatot, hanem annak kötődéseit szükséges feltérképezni olyan részletességgel, hogy ilyen módon vizsgálható, kiértékelhető legyen. Ezen kívül szükségszerűen a modellezéshez valamilyen további eszköz szükséges. A GRC (Governance, risk and compliance, irányítás, kockázatok és megfelelőség) ezen kutatások feltörekvő, növekvő területe és kiemeli, annak interoperábilis jellegét, hogy a megoldáshoz szükséges figyelembe venni az információs rendszereket, az üzleti szoftverfejlesztést, a jogi, kulturális és viselkedéstanulmányokat, valamint a vállalatirányítást is. Rosemann et al. (2005) a kockázatot minden üzleti folyamat velejárójának tekinti. Kliem (2000) pedig emberi, management és technikai kockázatokra osztályozza. Davenport rámutat a szervezeti/emberi erőforrásokra és az információs technológiákra, mint a folyamatinnováció két fő tényezőire (Davenport 1993). Ez azt jelenti, hogy a folyamatinnovációt lehetővé tevő tényezők negatív hatást gyakorolhatnak a vállalkozásokra, ha nem irányítják őket megfelelően. Napjainkban a GRC területen a tervezési megfelelőség elérésére érdekében megfigyelhető, hogy az üzleti folyamatmenedzsment (BPM) platformokat alkalmaznak. Ezek ideális eszközt jelenthetnek egy ilyen modellvezérelt megközelítéshez.

Fontos, hogy ez a fogalom, a nemmegfelelőség (ISO szabvány, 6.2 pontja) eltér a hiba (ISO szabvány, 6.3 pontja) fogalmától. Azaz a nemmegfelelőség hatékony feltárása érdekében meg kell fontolni, hogyan lehetséges annak észlelése: a) azon a területen ahol van mérés, de nem mutatja ki, b) nincs mérés.

A megfelelőségtől való távolság, vagy compliance distance pontos kereteinek meghatározásához szükséges a következő fogalmak bevezetése, illetve meghatározása.

Compliance set, vagy megfelelőségi halmaz: amely a belső szabályzatok és külső törvényi megfelelőség érdekében figyelembe kell venni, ide tartoznak még az iparági jó gyakorlatok, például, de nem kizárólag: ISO, NIST, ISA, stv.

Time dimension, vagy időbeli sík: amely arra tartalmaz előírást, (javaslatot, vagy kötelező érvényűt), hogy milyen sűrűn kell ellenőrzést lefolytatni.

További módosító körülmények lehetnek:

Hogyan kell lefolytatni az ellenőrzést és szükséges-e, milyen feljegyzés az elvárt.

A szabály alkalmazás gyakorlatától való eltérés előfordulása: esetszám, gyakoriság.

Esetszám vonatkozásában: relatív esetszám, abszolút esetszám, ismétlődés gyakorisága, balanced scorecard, elfogadott határérték alkalmazása.

Kutatásaim során azonosítottam egy olyan lehetséges tényezőt, amely az információbiztonsági kockázatfelmérés, az információbiztonsági tudatossági szint hatékony indikátora lehet. Ezt nemzetközi és magyar szakirodalomban nem szereplő területet a compliance (compliance check distance) vagy megfelelőség távolság neveztem el, amely úgy jellemezhető, hogy az ellenőrzés alá vett területek (szerepek) gyakoriságával jellemezhető érték. Ez úgy értékelhető ki, hogy az esetleg hosszabb ideje nem vizsgált, a rendszeres auditba be nem vont területeken vagy bevont, de nem megfelelően, vagy más fókusszal végzett mérés miatt akár – évek alatt – az információbiztonsági szabályzathoz mérve nagyobb mértékű eltérések, egészen megdöbbentő gyakorlat alakulhat ki, amely a megfelelőség (compliance) jó gyakorlattól való jelentős eltérés jellemezheti. A compliance check distance miatt pedig az adott szerepkörben dolgozó munkavállalók saját folyamatokban dolgozva nem kapnak visszacsatolást, így nem is érzékelik a jó, vagy ajánlott gyakorlatoktól való eltávolodást.

A fent említett, a folyamatokat mélységében feltáró és megértő megközelítés segítheti a compliance és biztonsági szakterületet kockázatok változásának érzékelésében.

Kutatásom során, ahogy bemutattam, a modellem alapján kidolgozott jelenléti oktatásokat tartottam. És bár az előadások során is az „A” vállalatnál alkalmazott jelenléti oktatásnál voltak kérdések, biztosított volt a kérdésfeltevés lehetősége. Ezek megfigyeléseim alapján mindig szorosan az adott témához, bemutatott részhez, viszonylag arra fókuszáltan érkeztek. Azonban az előadást követően biztosított ’kérdések és válaszok’ blokkban a kérdések jelentős része már nem szigorúan véve egy-egy részre koncentrált. Hanem a kérdések két fő, két nagyobb csoportba sorolhatóak. Az egyik az oktatás során bemutatottak, az elvárások saját munkafolyamataikban való alkalmazhatóságának kérdései, azzal való ellentmondások, azokra történő rákérdezés, tisztázó pontosító kérdések. A másik pedig az ezen szabályok, mint a magánéletben is javasolt gyakorlatok alkalmazására vonatkoztak. Ilyen visszajelzésre az e-learning esetében nem volt lehetőség. Bár a jelenléti oktatás keretében részt vettek és az e-learning kurzusokat elvégzettek száma összemérhető nagyságrendjét tekintve (3000 – 4000), azonban az e-learning oktatást követően nem érkeztek kérdések. Bár a klasszikus, az „A” vállalatnál bevettnek számító

elektronikus csatornák rendelkezésre álltak. Kutatásomnak nem tárgya, nem vizsgáltam az előadásokat követő csoportnyomást, azaz, hogy ha más sem kérdez, akkor senki sem kérdez, én se kérdezek érvényesült volna-e. Ugyanakkor míg a jelenléti oktatás során az első kérdéseket jellemzően tucatnyi követte, ahogy azt az előadások utáni kérdésblokkok hosszánál bemutattam. Az e-learningnél, általam nem vizsgált tényezők miatt, de nem éltek a kérdésfeltevés lehetőségével. A pontosság kedvéért meg kell említeni, hogy mind az „A", mind a „B" vállalatnál volt egy olyan intervallum, amikor még nem állt rendelkezésre írott szabályzat, illetve egy olyan intervallum, amikor 'csak' írott szabályzat állt rendelkezésre. Mind az „A", mind a „B" vállalatnál elenyésző számú, vállalatonként 10 alatti darabszámú kérdésfeltevés érkezett a szabályzat kiadását követően valamilyen elektronikus csatornán. Ahogy disszertációmban bemutatom a szabályzat olvasottságát, látogatottsági statisztikáját, feltételezhető, hogy annak alacsony ismertsége is hozzájárult ehhez. Az e-learning esetében pedig véleményem szerint az a kezdő lökés hiányzott, ami a jelenléti oktatásnál az első kérdező ad meg, ezeket azonban mélyebben nem vizsgáltam.

Ugyanakkor mindezek alapján a bemutatott számosságok alapján arra következtetek, hogy a jelenléti oktatás során kapott visszajelzések a bemutatott első csoportba soroltak, amelyek a munkafolyamataikban való alkalmazhatóságának kérdései, azzal való ellentmondásokra kérdeztek rá, jelentik az igazi értéket a biztonsági szakterületnek. Ezekre rákérdezve, feltárva lehet a nemmegfelelőségek észleléséhez inputokat szerezni, ezen visszajelzésekből. Ilyenkor történik meg voltaképpen az ismertetett szabályzat, szervezeti elvárás ütköztetése az egyes fejekben a saját hétköznapokban alkalmazott munkafolyamataikkal. Erről egyébként csak hosszadalmas kérdéslistákkal, személyes audit interjúkkal lehetne csak ilyen mélységű információt szerezni.

Erre az általam kidolgozott modell bizonyos esetekben megoldást nyújthat, mivel élő oktatás során a visszacsatolások megvalósulhatnak, általában véve a modell lényege a visszajelzés intézményesítése így az információbiztonsági szakterület képes lehet annak észlelésére, hogy az előírásoktól, az elmondott szabályoktól milyen távolság alakult ki, amennyiben azt visszacsatolják, hogy az adott munkakörben, szerepkörben területén az nem alkalmazható

5. KÖVETKEZTETÉSEK ÉS JAVASLATOK, VALAMINT ÚJ ÉS ÚJSZERŰ TUDOMÁNYOS EREDMÉNYEK MEGFOGALMAZÁSA

Disszertációm ezen fejezetében bemutatom, hogy milyen következtetéseket vontam le kutatásaimból, statisztikai elemzéseimből, megfigyeléseimből. Megfogalmazom javaslataimat, amelyek használatával, gyakorlatba ültetésével azt gondolom, hogy nemcsak kizárólag a közigazgatási információbiztonsági szakemberek, de minden közigazgatási munkavállaló támogatható. Ezen keresztül pedig a teljes közigazgatás vagy országos, szintű változások is elérhetőek. Végül az *Új és újszerű tudományos eredmények* részben (5.3) összefoglalom a modell alkalmazása során szerzett tapasztalatokat és azokat az eredményeimet, melyeket, bízom benne, hogy az elérhetőségük révén és a szakemberek által történő megismerést követően előbb-utóbb átültetnek a gyakorlatba, felhasználhatóvá válnak.

5.1 KÖVETKEZTETÉSEK

Ebben az alfejezetben a saját vizsgálataimból levont következtetéseket ismertetem az eddigiekben is használt logikai felépítés mentén, azaz hipotézisenként haladva mutatom be azokat.

Első hipotézisem alapján a közigazgatási szférában – összevetve az üzleti szférával – lemaradás tapasztalható az információbiztonsági tudatosság tekintetében.

A tudatosság mérésére a jelszóhasználati szokások kérdőíves felmérését választottam. A jelszó (általánosságban) mint hitelesítési eszköz kiváló indikátora az információbiztonsági tudatossági szintnek, a szabályalkalmazási gyakorlatnak azáltal, hogy kvantifikálható, mérhető, összehasonlítható. Az információbiztonság tekintetében felmerülő bizalmasság, sértetlenség, rendelkezésre állás közül többet, de legalább a bizalmasságot tipikusan valamilyen hozzáférési kontrollal, valamilyen hitelesítést biztosító eszközzel, például jelszóval valósítják meg. Széles körben elterjedt a hitelesítési eszközök használata, talán kijelenthető, hogy nincs olyan hely, ahol ilyet nem alkalmaznak – talán csak publikus információk esetében. Ezért a jelszó alkalmas mind a széleskörű felmérésre, mind pedig – kvantifikációja révén – idősoros mérési pontok előállítására, változása révén az információbiztonsági szabályok alkalmazási gyakorlatában történő változás nyomon követésére. Valamint rendelkezésre álltak már Som-Papp (2015),

valamint Tihanyi (2013) eredményei is, amelyek arra utaltak, hogy a jelszóhasználat alkalmas a vizsgálatra.

Az eddigi kutatási tapasztalatok (Illéssy, Nemeslaki, Som, 2014) rámutattak, hogy az interjús vizsgálatok során az interjúalanyok próbálnak megfelelni a feltett kérdésnél a feltételezett jó válasznak. Valamint az is belátható, hogy a jelszavakat nem lehet közvetlenül megvizsgálni, elemezni annak bizalmassága miatt. Így a kérdőíves módszer a legalkalmasabb arra, hogy egy viszonylag bizalmas információt mégis nagy számban lehessen vizsgálni, elemezni.

Az információbiztonsági tudatosság szintjének, illetve gyakorlatban történő alkalmazhatóságának mérésére tehát készítettem egy jelszóhasználati szokások felmérésére vonatkozó kérdőívet. A jelszó kiváló indikátora lehet az információbiztonsági gyakorlat kvantifikálásának. Ezen kérdőív 3 blokkot tartalmazott (demográfiai, információbiztonsági és IKT-jártasság szerinti felosztásban), ezt 1243-an töltötték ki. Az online kérdőív kitöltésére 2014 decemberétől 2015 júliusáig volt lehetőség. Az általam online megkérdezett 1243 válaszadó közül 384 fő a közszférából érkezett, valamint 358 fő az üzleti szférát jelölte meg. 490 fő nem jelölt meg szférát, s civil szférából 5 válasz érkezett. A közigazgatásban dolgozó kitöltők mintegy 35%-a férfi, 65%-a pedig nő volt. Az üzleti szférában dolgozó kitöltők mintegy 16%-a nő és 84%-a férfi volt. Ez számomra azt mutatja, hogy a mérés a nemek eloszlása alapján reprezentatívnak tekinthető, ha figyelembe vesszük a foglalkoztatottsági adatokat a közigazgatásban.

Ismerve a közigazgatásban alkalmazott információs rendszerek viszonylag nagy számát, valamint a válaszadók által megadott információs rendszerek számát, a válaszok alapján egyértelműen megállapítható, hogy kevés, kis számú különböző jelszót használnak a közigazgatásban dolgozó válaszadók. Könnyen belátható, hogy a hétköznapi élet során jellemzően 5-nél több különböző információs rendszert használunk, így mindenképpen kevés, ha ezen rendszerekhez 5 vagy annál kevesebb egyedi jelszó kerül alkalmazásra, illetve ebből következik, hogy egy vagy több információs rendszerhez ugyanaz a jelszó kerül újrafelhasználásra, ami komoly biztonsági kockázatot jelenthet.

A jelszót mint indikátort kezelve az is látható, hogy a jelszóval kapcsolatos *mennyiségi* elvárások nem feltétlenül teljesülnek: A közigazgatási mintát vizsgálva az átlagos jelszódarabszám 9.34 darab. Az üzleti szférát vizsgálva az átlagos jelszódarabszám 23.42 darab. Azt kaptuk eredményül, hogy a jelszóval kapcsolatos *minőségi* elvárások sem teljesülnek: hosszuk, bonyolultságuk, egyediségük, valamint darabszámuk nem elégséges. Ezen tényezők mindegyike külön-külön is jelentős kockázatot jelent. Összességében pedig a szabály vagy szabályozás ismeretének hiányát vagy annak meg nem értését, el nem fogadását jelentheti, a szabályalkalmazás gyakorlatának sérülését mutatja. Feltételezhető, hogy a válaszadóknak így

nincs ismeretük a helyes, jó, követendő gyakorlatról, illetve az üzleti szférával összevetve komoly eltérés tapasztalható: a közigazgatási értékek rendre lemaradtak. Az információbiztonsági szabályzatok ismeretére vonatkozó kutatási kérdéseim és megfigyelésem is azt támasztják alá, hogy a szabályzat önmagában nem elegendő a megfelelő tudatosság, gyakorlat kialakításához.

Mivel az információbiztonság bizalmassági tényezőjét alapvetően befolyásolja a jelszó hosszúsága, így egyértelműen kockázatot jelent a rövidebb, kevésbé komplex jelszó. Akár egy-egy karakterrel hosszabb jelszó is jelentős eredmény lehet, illetve jelentősen javíthatja a jelszó bizalmasságot biztosító paramétereit. Az általam végzett kutatás szerint a közigazgatásban és az üzleti szféra összehasonlításában (lásd 29. ábra) a jelszó hosszúságban mért 64,75%-os eltérés oka, hogy az üzleti szférában az átlagos jelszóhosszúság 7 karakterrel nagyobb a közigazgatásihoz képest, azaz jelentősen jobb gyakorlatot feltételez. Ha csak a jelszó hosszát vizsgálnánk visszafejthetőség szempontjából, akkor ez a paraméter a jelenleg ismert számítási kapacitások mellett igen jelentős különbséget jelent.

A jelszókezelést, annak gyakorlatát az információbiztonsági tudatosság, a szabályalkalmazási képesség egyik indikátorának tekintettem. A kiértékelés során indexet készítettem a skálás válaszadási lehetőségek egyik csoportjából. Nyolc változót azonos súllyal szerepeltettem a jelszókezelés-információbiztonsági tudatossági indexben, egy esetben pedig transzponáltam a kapott válaszok értékeit, mivel az állítás (*Ritkán változtatok jelszót.*) tagadó logikai minőségű volt, illetve információbiztonsági szempontból az egyet nem értés az elvárt attitűd. Ebből a nyolc változóból, annak kiértékeléséből készítettem indexet. Ennek eredményeképpen a közszférában 4,33-as átlagos értéket kaptam, míg az üzleti szférában ennél valamivel magasabb átlagos értéket, 4,38-at kaptam az aggregáltindex-értékre. Ezzel kapcsolatban fontos kiemelni, hogy mivel összesített indexről van szó, ezen eltérés is rendkívül jelentősen reprezentálja, hogy a közigazgatási érték alacsonyabb.

Az üzleti és közigazgatási szféra komplexebb összehasonlítása érdekében statisztikai próbákat végeztem. A beérkező adatok feldolgozásához az IBM SPSS statisztikai programcsomagját alkalmaztam. A Mann-Whitney próba szignifikáns eredménye ($p<0.05$) alapján jelentős eltérés igazolható az üzleti és közszféra dolgozói között az információbiztonsági tudatosságban. Az üzleti szférában jelentősen több és hosszabb jelszót használnak a közszférához képest, valamint itt kevésbé jellemző, hogy az új jelszó hasonlít a régihez.

Ezen kívül a khi-négyzet próba szignifikáns eredménye ($Chi2=69.456$, $df=1$, $p<0.001$) alapján jelentős eltérés igazolható az üzleti és közszféra között a személynevet tartalmazó jelszó előfordulási arányában: a közszférában dolgozók jelentősen nagyobb arányban rendelkeznek

ilyen jelszavakkal. Ez egyrészt alátámasztja hipotézisem, másrészt arra utal, hogy a szabálytudás vagy szabályalkalmazás gyakorlata elmarad.

Továbbá a változókon elvégeztem a khi-négyzet próbát, amelynek szignifikáns eredménye (Chi2=13.534, df=1, p<0.001) alapján jelentős eltérés igazolható az üzleti és közszféra között abban is, hogy van-e olyan szó, név, kifejezés, amelyik több jelszóban is előfordul: a közszférában dolgozók jelentősen nagyobb arányban rendelkeznek ilyen jelszavakkal.

Ezt követően a közigazgatási információbiztonsági kérdőív elemzésére tértem át a hipotézisem további vizsgálatához. A kutatást társaimmal, Illéssy és Nemeslaki kutatókkal közösen 2013 decembere és 2014 februárja között végeztük el; 379 fő vett részt kitöltőként, közülük 285-en válaszoltak minden kérdésre. A későbbiekben interjúkkal is árnyaltuk a kapott válaszokat.

A kérdőívek alapján elmondható, hogy a budapestiek nagyobb arányban szerepeltek a kitöltők között, ők feltehetően eleve nagyobb tudatossággal rendelkeznek, és munkahelyeik esetében is nagyobb eséllyel feltételezhető, hogy gondot fordítanak az elektronikus információbiztonsági szabályok betartására, illetve számos közigazgatási szervezet jellemzően budapesti székhellyel rendelkezik.

Életkor szerint a legfiatalabbak teljesítettek ugyan a legjobban, azonban a 35-44 éves korosztály törést mutat, náluk a mintában képviselt súlyukhoz képest jelentősen nagyobb arányban találunk relatíve rosszabb értékeket, mint akár a náluk fiatalabbaknál, akár a náluk idősebbeknél. A válaszadók 88%-a nyilatkozta, hogy van informatikai biztonsággal foglalkozó részleg a munkahelyén. A felhasználók számára sok esetben nem különül el élesen az informatikai és információbiztonsági szervezeti egység, a feladatkör vagy a szabályzat. Ez az állítás köszön vissza a TAM modellnél is, valamint az IKT-képességekkel kapcsolatos értékek is ezt igazolják.

A felhasználók közel 15%-a találkozott már valamilyen vírussal, kártékony kóddal a saját munkafolyamatai során. Így az információbiztonsági kutatás, vizsgálatok jogosságát igazolja ez is; eszerint információbiztonsági incidenseknek erősen kitett szektorról beszélünk.

Az *Ön szerint észrevenné-e, ha számítógépét feltörnék vagy megfertőződne?* kérdésre adott válaszok azt mutatják, hogy a felhasználók azt feltételezik, hogy valamilyen módon azonnali vizuális, észlelhető hatása van annak, ha a számítógépük, információs rendszereik kompromittálódnak. Az elmúlt évtizedben megfigyelhető változások alapján viszont ez jellemzően nem társul azonnali vagy látványos eseményekkel. Éppen ezért fontos a biztonságtudatos magatartás akkor is, ha látszólag nincs azonnali hatás.

Megadta-e már céges jelszavát másnak? – erre a kérdésre a 367 válaszadó közül 174, azaz 47,41% válaszolt igennel, azaz általános jelenséggel van dolgunk, amelyet tovább árnyalhat a

csoportnyomás jelensége. Ugyanakkor nem csak önkéntes vagy önkényes megoldásról van szó, hanem vélhetőleg a munkafolyamatok nem megfelelő kialakítása, felmérése és az információbiztonsági szabályzatok kialakítása során figyelembe nem vett tényezők együttesen vezetnek ilyen gyakorlatokhoz. Tehát rendszerszintű problémára utalnak. Ez egy kiemelkedően jó példa a compliance distance jellegű kockázatok érzékelésének hiányára.

Az elemzésem során többször rámutattam, hogy a személy magánéleti információbiztonsági és a munkaszervezetben tanúsított információbiztonsági viselkedése kongruens kell, hogy maradjon. A magánéletben és munkaszervezetben is alkalmazott technológiák szabályalkalmazási gyakorlatát azzal is lehet támogatni, hogy mindkét területen bemutatásra kerülnek a jelentkező kockázatok.

Az Illéssy, Nemeslaki, Som (2014) kutatás interjúi során a megkérdezett szakértők többsége arról számolt be, hogy Magyarország lemaradásból indult az információbiztonsági szabályozás területén. A lemaradás azonban nem feltétlenül információbiztonsági szakmai szempontokra vezethető vissza, hanem talán a kötelező érvényű szabályozásban és az ajánlásban mint nem kötelező érvényű, de akár költségekkel is járó tényezőben kereshető az az információbiztonsági ajánlások alkalmazásában, elterjedésében a különbség. A 2013. évi L. törvény[11], majd az azt követő 41/2015. (VII. 15.) BM rendelet[12] már nem "csak" ajánlás. Ugyanakkor – a megszólított szakértők szerint – hiába indultak el a 2013-as években egyébként is egyértelműen pozitív folyamatok, ahhoz, hogy ennek érezhető hatása legyen, még időre lesz szükség. Idő, amíg a változás a szervezetekben, folyamatokban, a munkaszervezeti kultúrában is megjelenik.

Mindezen következtetéseket egybevetve **megállapítottam, hogy az információbiztonsági tudatosság szintjének tekintetében a magyar közigazgatás területén lemaradás tapasztalható a magyar üzleti szférával összehasonlítva, azaz a H1-t elvetettem.**

A második hipotézisem (H2) szerint az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest, amihez a bejelentési esetszámot mint indikátort hívtam segítségül.

Egy budapesti székhelyű közigazgatási munkaszervezetben kérdőív segítségével kérdéseket tettem fel többek között az információbiztonsági szabályzatra vonatkozóan. Arra a kérdésre, hogy *Ön szerint hány oldal terjedelmű az informatikai szabályzat?*, a 10 oldal és a 150 oldal között lehetett választani 8 lehetőség közül. Helyes választ mindössze 3 fő adott, (24

[11] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról

[12] 41/2015. (VII. 15.) BM rendelet az állami és önkormányzati szervek elektronikus információbiztonságáról szóló 2013. évi L. törvényben meghatározott technológiai biztonsági, valamint a biztonságos információs eszközökre, termékekre, továbbá a biztonsági osztályba és biztonsági szintbe sorolásra vonatkozó követelményekről

válaszadóból), mivel a szervezet akkor hatályos IBSZ-e 107 oldal terjedelmű volt. Az adott munkaszervezet információbiztonsági szabályzatát nem ismerik, terjedelmét hozzávetőlegesen sem tudták megbecsülni. A szervezetben ezt megelőzően tantermi információbiztonsági oktatás nem volt. A gyakorlat szerint a szervezetnél a szabályzatot elérhetővé tették az intraneten, és az éves kötelező vizsga is az intranet oldalon volt elérhető. A vizsga fix kérdéseket tartalmazott, azaz a kérdések és helyes válaszok mindenkinél azonosak voltak a munkaszervezetben. Egyes vélemények szerint a megoldókulcs ismert volt a munkavállalók körében. Ebből következően lemaradásként értékelem, hogy ha a közigazgatási szervezet munkavállalói nem ismerik, hogy milyen információbiztonsági szabályok és elvárások vonatkoznak rájuk, vagy hogy ezeket az elvárásokat honnan ismerhetik meg, hol tájékozódhatnak azokról. Mindezek alapján arra lehet következtetni, hogy az írásbeli információbiztonsági szabályzat nem ismert a munkaszervezetben, mivel a munkavállalók az IBSZ hozzávetőleges nagyságát, oldalszámát sem ismerik, annak tartalmáról, elérhetőségéről sem rendelkeznek információval; a pusztán elérhető vagy az online mindössze elérhetővé tett szabályzat nem jutott el a munkavállalókhoz, vagy azt nem nyitották meg, annak helyét és tartalmát nem ismerték.

Disszertációmban voltaképpen azokra a mély miértekre és gyökérokokra próbálok rávilágítani, amelyeknek megértése és feltárása alapja lehet egy olyan transzformációnak, amire szükség van a szokások és mélyben megbúvó, alattomos, rossz gyakorlatok, csoportnormák megváltoztatásához. Egyike ezeknek az információbiztonsági szabályzatok kiadásának menete, azok gyakorlatba való átültetéséhez nyújtott támogatás hiánya. Megfigyeléseim alapján a szabályzat olvasásakor, annak ismertetésekor, visszajátszott videós (nem élő) előadáskor vagy bármilyen olyan – általam megfigyelt egyéb – módszernél, ahol nem lehetséges a kérdésfeltevés vagy aktivizálódás, bevonódás, ott az elmondott szabályok még akár, ha szövegszerű állításokként meg is maradnak, memorizálódnak, és emlékezhetnek rájuk bizonyos esetekben, a gyakorlatba mégis kevésbé vagy nem tudnak beépülni.

Ezt követően indexet képeztem az alábbi kérdésekre adott válaszokból, és csoportosítási változónak a *Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?* kérdést állítottam be.

1. Hozzávetőlegesen hány darab különböző jelszót használsz?
2. Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?
3. Milyen sűrűn változtatod meg (általában) a jelszavaidat?
4. Hány karakter a leghosszabb jelszavad?
5. Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?
6. Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, vagy eléggé hasonlít a régi jelszóhoz?

Ezen értékeket a Mann-Whitney Testnek vetettem alá. Az üzleti szférában csak az azonosítók számában igazolható jelentős eltérés (M-W: Z=-3.028, p=0.002) az oktatásban részesült és abban nem részesült dolgozók között: az oktatásban részesültek jelentősen nagyobb számú azonosítóval rendelkeznek.

A közszféra esetében az azonosítók számán kívül a jelszavak számában is jelentős eltérés mutatható ki az oktatásban részesültek és abban nem részesültek között: az üzleti szférához hasonlóan itt is jelentősen nagyobb számú jelszóval és azonosítóval rendelkeznek az oktatásban részesültek.

Az oktatás hatását további kérdéseknél is megvizsgáltam, így a *Van-e olyan jelszavad, ami tartalmaz személynevet?* kérdést szféra szerint az oktatás függvényében vizsgálva azt az eredményt kaptam, hogy a khi-négyzet próba eredménye ($p>0.05$) nem szignifikáns, így nem igazolható jelentős eltérés az oktatásban részesültek és nem részesültek között a személynevet tartalmazó jelszó használatának gyakoriságában, sem az üzleti, sem a közszféra esetében.

A *Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?* kérdést is vizsgálva hasonló eredményt kaptam, ami a minta jóságát mutatja, együtt mozogtak ezen változók. A khi-négyzet próba eredménye ($p>0.05$) nem szignifikáns, így nem igazolható jelentős eltérés az oktatásban részesültek és nem részesültek között abban, hogy van-e olyan szó, név, kifejezés, amelyik több jelszóban is előfordul, sem az üzleti, sem a közszféra esetében.

Véleményem szerint a fenti két kérdésre kapott statisztikai próba eredményének az lehet az oka, hogy habár a megkérdezettek kaptak oktatást, de az oktatás nem terjedhetett ki sok esetben a jelszóképzési gyakorlatra – azt feltételezem, hogy csak a „klasszikus” *használj hosszú, használj jó jelszót* szabályismertetésre. Tehát a szabályalkalmazás gyakorlati megvalósításához nem kaphattak elegendő ismeretanyagot, tréninget.

A *Közigazgatási képzés előtt/után kérdőívet* egy budapesti székhelyű, országos érdekeltségű közigazgatási munkaszervezetben vettem fel 2013 szeptembere és októbere folyamán. A kérdőív kitöltése nem volt kötelező; az oktatás előtt 24, míg oktatás után 25 fő töltötte ki. Az elemzések során fény derült arra, hogy a *Safer Internet Programról* csak elvétve hallottak a válaszadók. A képzésen való részvétel sem volt kötelező, a válaszok alapján a kitöltők elsősorban magánéleti indíttatásból döntöttek a részvétel mellett. A válaszok jól mutatják a kontrasztot, hogy ha valami érdekes a munkavállaló számára, felkeltette az érdeklődését, úgy gondolja, hogy hasznos lesz számára a magánéletben vagy munkafolyamataiban, és arra minőségi és mennyiségi, dedikált időt szánt, akkor részt vett az oktatáson; míg az egyébként bármikor online elérhető szabályzat megismerését – amelynek ismerete egyébként kötelező – nem vagy kevésbé tartja fontosnak.

A vállalathoz tartozó tantermi képzés megkezdését követő havi bejelentési adatok eloszlása nem tekinthető normálisnak (Kolmogorov-Smirnov próba: t=0.299, p=0.011), ezért a kétmintás t-próba helyett az F próba mellett döntöttem. A varianciaanalízis jelentős eredménye (F=9.617, p=0.001) után elvégzett Dunett T3 post hoc próba igazolja, hogy a tantermi képzést követően a bejelentések száma jelentős mértékben növekedett mind az IBSZ publikációt követő szakaszhoz, mind a szabályozás előtti szakaszhoz képest.

Fontos tehát a hatékonyság megértése az információbiztonsági oktatások szempontjából. Nem elég tudni a szabályokról, hanem mélyen hinni kell bennük, megérteni, hogy az egyén érdekeit, a munkáltató érdekeit védik, és ha azokat nem tartják be, akkor lehet, hogy egy komoly incidens miatt akár a munkahely is, illetve annak reputációja is veszélybe kerül.

Hipotézisem alátámasztása érdekében szerencsém volt két külön munkaszervezetnél is vizsgálatot végezni, azaz a kiadásra kerülő IBSZ (információbiztonsági szabályzat) és IBP (információbiztonsági politika) kihirdetése előtti és utáni trendek vizsgálatára nyílt lehetőségem. Ezen intervallumok, azaz az információbiztonsági szabályzat kihirdetése előtti, majd az azt követő értékek, valamint a jelenléti oktatást megelőző és az azt követő trendek szignifikáns eltérést mutattak.

Összegezve tehát **megállapítottam, hogy az információbiztonsági szabályalkalmazás gyakorlata jelenléti oktatás keretében hatékonyabban fejleszthető az írásbeli szabályozáshoz képest, azaz a H2 hipotézisemet elfogadottnak tekintettem.**

Ezt követően ***a harmadik hipotézisemből*** (H3) kiindulva azt vizsgáltam meg, hogy az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető-e. Kimutatható-e az általam választott indikátor segítségével a szignifikáns változás.

Az e-learning oktatás értelmezésemben és az általam alkalmazott kutatáson belül azt jelentette, hogy kifejezetten e-learning szerkesztő eszközzel készült, elágazásokat tartalmazott. A fejlesztés során arra helyeztem a hangsúlyt, hogy az alapvetően nem élőszereplős, nem élő előadáshoz képest a modellem egyes részeit, ahol csak lehetett, alkalmazzam, prezentációm a lehetőségekhez képest minél interaktívabb legyen, a színek, formák, példák mind illeszkedjenek az adott tartalomhoz. Ahol lehetséges volt, a figyelem további fókuszálása érdekében színezést, kiemelést alkalmaztam. Jellemzően minden dián valamilyen további interakció volt elvárt, nem lehetett „csak” olvasással továbbhaladni vagy átpörgetni. A grafika, a színvilág, a piktogrammok, ikonok igazítása is szempont volt. Ugyanakkor alapvető cél volt, hogy megvalósuljon a figyelem, a fókusz irányítása egy kibertámadás során felismerhető, felismerendő, tipizálható elemekre.

Az e-learning megoldás során a SCORM csomagba importálható, így tetszőleges LMS rendszerben lejátszható. A vizsgálat során a Moodle rendszert alkalmaztam, mivel az adott

vállalatnál az állt rendelkezésre. Az e-learning kurzusok intranethírként, nem kötelező tananyagként kerültek meghirdetésre. (Pont úgy, ahogy a szabályzatok publikációja történt.)

Az *E-mail biztonsági alapok* e-learning kurzusnál a sikeres teszthez 80%-os eredményt kellett elérni. A 2853 kitöltési próbálkozás 2196 egyedi személyhez tartozott. Az e-learninghez kapcsolódóan, de attól különállóan publikált kérdőívet 902 egyedi válaszadó töltötte ki, értékelte a képzést egy ötfokozatú skálán, valamint megjelölte, hogy miért találta azt hasznosnak.

A *Jelszóbiztonság kezdő szinten* című e-learning tananyaghoz tartozó tesztet 1976 egyedi kitöltő kezdte el megoldani, 2902 darab próbálkozás történt. A sikeres teszthez 75%-os eredményt kellett elérni.

Az e-learninghez kapcsolódóan, de attól különállóan publikált kérdőívet 901 egyedi válaszadó töltötte ki, értékelte a kurzust egy ötfokozatú skálán, valamint megjelölte, hogy miért találta azt hasznosnak.

Az *Adathalász támadások elleni védekezés lehetőségei* című e-learning tananyaghoz tartozó tesztet 2667 egyedi kitöltő kezdte el megoldani, 3454 darab próbálkozás történt. A sikeres teszthez 70%-os eredményt kellett elérni. Ehhez a tananyaghoz nem készült visszajelzésmodul.

Vizsgáltam az információbiztonsági szabályzat kiadása előtti, utáni és az e-learning publikáció előtti és utáni időszakokat, a felhasználói bejelentések számával való összefüggést. Statisztikai próbák alapján nem volt kimutatható jelentős eltérés ($F=1.126$, $p=0.303$) a szabályzatpublikáció és az e-learning képzés között a bejelentések számában. A szabályozás nélküli szakaszhoz képes nem vizsgálható az eltérés, mert nincs elegendő adat.

Bár statisztikai próbákkal nem volt kimutatható korreláció, ugyanakkor hangsúlyoznám, hogy miért is kiemelkedő jelentőségű ezen megfigyelésem. A teljes szabályzattár átlagosan havi 400-as megnyitásával szemben itt a többezres megtekintés mellett ezres nagyságrendű önkéntes tanulás, majd feladatmegoldás és ezres nagyságrendű visszajelzés volt mérhető. Valamint az önkéntesen, saját belső indíttatásból elvégzett e-learning modul kapcsán a nagyságrendileg háromezer fő által elvégzett tananyagot követően önkéntesen vizsgát tettek, azt esetenként többször javították, újra elvégezték, és a szintén önkéntes visszajelzésre alkalmas kérdőívet is magas százalékos arányban töltötték ki.

Az e-learning kurzus feladatainak kitöltését követően a vizsgázóknak lehetőségük volt visszajelzést adni, ami nem volt kötelező. A válaszadók 78,075%-a jelölte meg az *Új szempontokra hívta fel a figyelmemet, ha növelni akarom adataim biztonságát.* opciót. Az *Értékelje egytől ötig terjedő skálán, hogy mennyire volt hasznos az Ön számára a tanfolyam! (1 = nem volt hasznos, 5 = nagyon hasznos volt)* pontnál 886 kitöltő adott számszerű értékelést, melyek átlaga 4,49 volt.

Ezt összevetve az élő előadásokat követő kérdezési lehetőséggel az látható, hogy a 90 perces előadás után az átlagosan 20 perces további kérdésblokkot igénybe vette a résztvevők egy része. Az előadás utáni kérdésfeltevés lehetőségét igénybe vevők számáról nem készült pontos kimutatás, mivel a pontos számosság meghatározását nehezítette, hogy ez a szám a kérdésblokk végéhez közeledve folyamatos csökkenést mutatott, nem pedig két konkrét értéket vett, vehetett csak fel. Tapasztalataim szerint nagyságrendileg 5% és 35% között változott az előadás után tovább maradók számossága.

Összegezve tehát **megállapítottam, hogy az információbiztonsági szabályalkalmazás gyakorlata e-learning oktatás keretében fejleszthető, ugyanakkor ennek eredményeit összevetve az írásbeli szabályozásnál mért eredményekkel, a különbség statisztikailag nem kimutatható szignifikánsan, azaz a H3 hipotézisemet elvetettem.** Ugyanakkor kiemelkedő jelentőségűnek tartom, hogy a modellem alapján megtervezett és kivitelezett, javaslataim alapján összeállított (nem kötelezőnek, hanem érdekesnek, magánéleti vetületben is alkalmazhatónak kommunikált) oktatási tananyagokat (3 db) nagy volumenben dolgozták fel önkéntesen a résztvevők. További mérések és vizsgálatok keretében érdemes lenne annak kutatása, hogy milyen jelentősége van, hogy az itt óvatosan bevezetett szakszavakra építkezés milyen módon gyorsítja, támogatja, teszi jobban befogadhatóvá a szabályalkalmazási gyakorlat további fázisait. Továbbá lehetséges annak vizsgálata, hogy szükséges-e más indikátort választani vagy egyéb kérdőíves felmérést végezni a jövőben.

5.2 JAVASLATOK

Ebben a fejezetben a kutatási eredmények és azok értelmezése alapján a több évet átfogó számos kutatás és megfigyelés alapján felmerült jobbító, fejlesztő szándékú javaslatok kerülnek megfogalmazásra. Ez lehetővé teheti más közigazgatási vagy egyéb szektorban dolgozó információbiztonsági szakemberek számára nemcsak a kutatási eredmények megértését, hanem a megkezdett munka átültetését a saját munkaszervezetükbe vagy annak továbbfejlesztési lehetőségét is.

Azt gondolom, nem lehet kevesebbet célként kitűzni, mint azt, hogy Magyarországon a közigazgatáson keresztül nemzeti szinten, azaz nem kizárólag csak a magyar közigazgatásra, de áttételesen akár más szférára, Magyarország közigazgatási területén belül nemzeti szinten lehetővé váljon az információbiztonsági tudatosság emelése. Ennek számos vetülete van: az álhírek felismerése, a megtévesztő levelek felismerése, különböző csalási formák felismerése.

Jelentős az a fenyegetés, amit az álhírek, dezinformációk, médiaműveletek, különböző információs rendszereken keresztül történő támadása jelent.

Az állami szolgáltatásokba vetett bizalom (Som et al., 2015) országos, az e-szolgáltatásokba, e-kereskedelembe vetett bizalom pedig nemzetgazdasági érdek. (Papp-Som, 2015) Tekintve, hogy Magyarországon a közigazgatás az egyik legnagyobb munkáltató, így ezen a szférán keresztül áttételesen a munkavállalók családtagjai is elérhetőek lehetnek. (A csoportnyomás jelensége, valamint az *Információbiztonsági indikátor* kérdőív információk szerzésére vonatkozó kérdésére adott válaszok ezt alátámasztják.)

Javaslatom egy központilag koordinált, tudományosan támogatott, meglévő vagy új szervezethez rendelni az információbiztonsági tudatosság mérését, kiértékelést, fejlesztését, és ezt követően nemzeti szinten meghatározni a fejlesztendő területeket. Ezáltal a közigazgatásban dolgozó információbiztonsági szakemberek jelentős támogatást kaphatnának a heti-havi kommunikációhoz plakátok, hírlevelek formájában.

Illéssy, Nemeslaki, Som (2014) is megállapította, hogy a 2013. évi L. törvény kiemelkedő alapokat teremtett, azonban azóta sem történt változás alapszinten sem, azaz szükséges a jelenlegi tudásszint és fejlesztendő területek meghatározása az érintett szervezeteknél. (Központi, közigazgatási vagy nemzeti szintű mérésről nincs tudomásom azóta sem.) Ahol ilyen történt, az szigetszerű, egymással össze nem vethető eltérő kérdőívek alkalmazásával, elszórtan történt. Ilyen országos szintű információ birtokában képessé válhat a közigazgatás a felmért kockázatokra hatékonyan reagálni, célzottan, geolokáció, életkor, szervezet stb. paramétereket is figyelembe véve.

Akár az NKE EIV-ben végzett, akár a 2013. évi L. törvény által lehetővé tett egyéb végzettséggel rendelkező információbiztonsági szakemberekről van szó, egyik területen sem kaptak az érintettek oktatási, didaktikai képzést. Javaslatom szerint szükséges lenne az információbiztonsági szakembereknek központilag és tudományos támogatással kialakított kommunikációs, oktatási, felmérési anyagok központi biztosítása. Ennek segítségével hatékonyabban tudnák ellátni oktatással és kockázatfelméréssel kapcsolatos feladataikat. Hatékony visszajelzést kaphatnak a saját szervezetükről. Az egyes elkészült felmérések központilag kiértékelhetőek és hatékonyabbak a más volumenben rendelkezésre álló információk által.

Az elért eredmények kiértékelése alapján pedig kiterjeszthető lenne az oktatási platform: az elérhető információbiztonsági oktatási anyagokat és szolgáltatásokat minden ügyfélkapus magyar állampolgárnak elérhetővé lehetne tenni, vagy szolgáltatásként elérhetővé lehetne tenni az üzleti szférának is.

Szorosabb együttműködésre lenne szükség azokkal a meglévő szervezetekkel, ahol az ilyen incidensek nagy tömegben jelentkeznek és észlelhetőek, mint például a Nemzeti Infokommunikációs Szolgáltató, a Készenléti Rendőrség Nemzeti Nyomozó Iroda Kiberbűnözés Elleni Főosztálya, a GovCert.

A modell és a megfigyelések alapján, valamint a számszerűen igazolt tényekből és tapasztalatokból és levont következtetésekből, azok miatt felmerült jobbító, fejlesztő szándékú javaslatok megfogalmazásán kívül fontosnak tartom, hogy ez a javaslat, információ eljusson az információbiztonsági szakemberekhez. Mindez más közigazgatási vagy egyéb szektorban dolgozó információbiztonsági szakemberek számára nemcsak a kutatási eredmények megértését teheti lehetővé, hanem magában foglalja a megkezdett munka átültetését a saját munkaszervezetükbe, vagy annak továbbfejlesztési lehetőségét is.

Az információbiztonsági tudatosság vállalatirányításba való beépítése és az ehhez szükséges keret elkülönítése javasolt a szervezetek támogatására az integrációs erőfeszítéseik során. Az információbiztonsági tudatosságot mérő eszköz fontossága tehát – a befektetés megtérülése, a biztonsági kampányok átirányítása stb. mellett – összekapcsolható a szervezet legmagasabb szintű vezetésével. Az információbiztonság és a menedzsment elválaszthatatlanok, és fontosak például az irányítási és az ellenőrzési szempontok. Ezek a szempontok a társaság igazgatótanácsának feladatai, és feladataik ellátása érdekében megfelelő vállalati és információbiztonsági irányítási keretrendszerre van szükségük; valamint visszajelzésre arról, hogy mi történik a vállalatban az információbiztonság szempontjából. Mi lehet alkalmasabb eszköz az információbiztonsági szakterület kezében ezen igények bemutatására, mint a megfelelő oktatási és visszamérési rendszer alkalmazása?

A kérdőív és a szakértői interjúk alapján javasolt központilag kiadni olyan általános segítséget, amelyet az adott területen tevékenykedő szervezetek be tudnak építeni a saját szabályozásukba. (Az éves kérdőíves felmérésekhez is javasolt ilyen központi ajánlás kiadása, vagy legalább a mérendő területek megnevezése az ajánlásban.) Ugyanakkor minél inkább javasolt ezen mérés központosítása és lehetőleg minél kisebb mértékű eltérések engedélyezése, hogy a mérési eredmények összevethetőek, kiértékelhetőek legyenek. Így bizonyos, minden munkaszervezetben tipizálható munkakörre tovább lehetne bontani a felmérést: alsó-, közép- és felsővezető, IT-üzemeltető stb.

Mivel az információbiztonsági oktatások megtartására vonatkozó törvény és a gyakorlat összehangolása nehézséget okoz, eltérő gyakorlatot eredményez, így megfontolandó ezen területen az egyértelműsítés, valamilyen központilag koordinált magas színvonalon tudományos igényességgel kidolgozott tananyagok és mérések koordinációja.

Amennyiben központilag koordinált módon gyűlnek adatok, akkor a kutatási eredmények gyakorlati felhasználása révén azonnal lehetővé válhat az információbiztonsági nemzeti jelenállapot (as-is state) meghatározása, rövid távon ezek révén meghatározhatóak a fejlesztendő területek. Középtávon a megfelelő változtatásokkal (súlyozott oktatás, didaktikai és kommunikációs képzés) és fejlesztésekkel (éves biztonsági kommunikációs csomag létrehozása) támogatni lehet az információbiztonsági pozícióban dolgozó munkavállalókat, ezekkel pedig a tudatossági szint emelését. Hosszú távon pedig a nemzeti kibertudatossági szint számos kapcsolódó területet képes lenne erősíteni, támogatni, példaként említve a közigazgatásba, az e-kapcsolattartásba, e-szolgáltatásokba vetett bizalmat, vagy a fake news vagy egyéb átverési kísérletek észlelésének és jelentésének jobb arányát is.

Javasolt továbbá, hogy a munkavállaló egyén magánéleti információbiztonsági és a munkaszervezetben tanúsított információbiztonsági viselkedése kongruens maradjon, valamint a biztosított támogatás túlnyúljon a szigorúan vett munkaszervezeti határokon. Terjedjen ki az oktatás a részben magánéleti területekre is, mivel azokon a határterületeken is azonosíthatóak kockázatok.

Javaslom az információbiztonsági szakembereknek, hogy lehetőség szerint valósuljon meg jelenléti vagy élő oktatás, ahol lehetőség van visszakérdezni, nyílt kommunikációt kezdeményezni. Az oktatások darabszámára nehéz ajánlást tenni, mivel az önmagában nem indikátor. A szervezetnek kell megvizsgálnia, hogy milyen lehetőségei és milyen kockázatai vannak. A lehetséges indikátor sokkal inkább a hatékonyság mérésében, az elért eredményekben rejlik. Azaz szükséges a megértés és szabálykövetés mérése, tesztelése vizsgáztatás vagy egyéb formában. Amennyiben nincs erre forrás, vagy ezt más akadály hátráltatja, megfontolható külső szakértőt, vendégelőadót hívni. Számos tényező indokolja, hogy nem elegendő évente egyszer oktatni, bármennyire is jó az oktatás és a tudásátvitel. Ennek indoka a disszertációmban részletesen kifejtett tanulási és felejtési görbe, amely alátámasztja, hogy ideális a tudásanyag időben történő megerősítése, annak szinten tartása érdekében. Bagchi (2003) szerint évente vagy sűrűbben jelentkeznek információbiztonsági incidensek. Változások, új kockázatok vagy új támadási formák, típusok és stílusok jelenhetnek meg. Ezek jellemzően nem igazodnak a naptári évhez vagy tervezett oktatási programhoz, így ez is indokolja, hogy ad-hoc, évközi oktatással reagáljon a szervezet a változásokra. Továbbá az egyes információbiztonsági képzési területek számossága is azt indokolja, hogy azok időben elkülönülten, de egy éven belül mindegyiket (vagy a meghatározottakat) érintve kerüljenek az oktatásba. (Könnyen belátható, hogy a szerteágazó területek számossága és a megtanítandó tudás, az alapfogalmak tisztázása, a téma ismertetése, majd annak begyakoroltatása, készségszintre emelése nem lehetséges egyetlen alkalomba

sűrítve.) Idő szükséges a tudás beépülésére, amíg az elmélettől a gyakorlatig megtörténik, készségszinten beépül a tudás.

Az információbiztonságiszabályzat-készítő és -fejlesztő, közigazgatási vagy más szektorban dolgozó szakemberek számára javaslom, hogy jelenjen meg a szabályzatban a kivételek kezelésének lehetősége és engedélyezett módja; valamint a szabályzat változása vagy bevezetése során annak ütemterve, úgymond a türelmi idő kérdésköre is.

Javaslom, hogy kerüljön be az alap-, a közép- és felsőfokú oktatásba az információbiztonsági szakterület. Kifejezetten azon egyetemi képzésekbe is, ahol a végzést követően a munkába állók fiatalkorúakkal foglalkoznak. Mivel ezen fiataloknak már internetes elérésre alkalmas eszközük, információs rendszerhez való hozzáférésük van, őket fokozottan kell támogatni, felkészíteni ezen események észlelésére. Ezen nevelői-oktatói munkakörben lévőket támogatni szükséges, hogy tudják, hova lehet fordulni támogatásért (kék szám, EU SIP stb.), vagy milyen bevált módszerek állnak rendelkezésre. Ugyanakkor Simonics (2007) rámutat azokra a kihívásokra, amelyek általában véve nehezítik az elektronikus tananyagok terjesztését és a pedagógusoknak szánt támogatás, továbbképzési lehetőség elérésének lehetőségét. Valamint Törley (2020) kutatása elsőéves egyetemista diákok információbiztonsági tudásának elemzése révén rámutat, hogy a terület fejlesztendő. Ezt szintén alátámasztja Roskó és Szőllősi (2021) középiskolások és egyetemisták körében végzett kutatása. Arra is szükséges utalni, hogy a jelszón mint az információbiztonság egyik lehetséges indikátorán túl az információbiztonság vagy adatvédelmi tudatosság számos területen szorul fejlesztésre. Roskó és Szőllősi (2021) ugyanakkor rámutat, hogy az oktatás kulcsfontosságú elem, kiemelve, hogy az internetet ma már alapvető információforrásként használják (Hopp és Sheehan, 2019, In: Roskó és Szőllősi, 2021). A barátok és kollégák adatvédelmi magatartása szintén fontos tényező (Boyd és Hargittai, 2010, In: Roskó és Szőllősi, 2021). Roskó és Szőllősi (2021) arra a következtetésre jut, hogy a felhasználók adatvédelmi tudatosságának fejlesztésére való oktatása kulcsfontosságú feladat a személyes kiberbűnözés jövőbeli növekedésének megakadályozása érdekében.

5.3 ÚJ ÉS ÚJSZERŰ TUDOMÁNYOS EREDMÉNYEK

1) **Felmértem az információbiztonsági szintet a magyar közigazgatási szférában.**

A szakirodalom áttekintése során fellelt információbiztonsági modellek, valamint többéves egyetemi és egyéb (SIP) oktatási tapasztalataim alapján kidolgoztam egy saját kérdőívet. Ezen kérdőív három részből áll: egy demográfiai, egy jelszókezelési, valamint egy IKT-jártassági

blokkból. Ezen kérdőív segítségével is bizonyítottam, hogy a jelszókezelési szokások (a jelszó mint hitelesítési eszköz kezelése) megfelelő indikátorai lehetnek az információbiztonsági tudatossági szint mérésének. Ennek segítségével részben azonosíthatóak az információbiztonsági kockázatok, a tudásszint és a szabálykövetési hajlandóság. A kérdőívet az azonosítással, jelszókezeléssel kapcsolatos releváns, kiemelkedő kockázatok azonosítására dolgoztam ki. Így a kockázatok azonosítása alkalmas lehet bármilyen közigazgatási információbiztonsági szakembernek későbbi hasznosításra, vagy széles spektrumban a teljes közigazgatásban egységesen alkalmazhatóvá tehető.

Az általam kidolgozott információbiztonsági kérdőív segítségével feltártam az információbiztonsági szintet a magyar közigazgatási szférában. A felmérést kiértékeltem, és megállapítottam, hogy a közigazgatási szférában az információbiztonsági szint (jelszóhasználat) tekintetében, mint ami az információbiztonság indikátora, lemaradás tapasztalható az üzleti szférával összehasonlítva.

A kérdőívet összesen 1243 fő töltötte ki az üzleti és a közigazgatási szférából. Likert skála, kvantitav értékek és szabadszavas mezők segítségével a kérdőívben demográfiai, információbiztonsági és IKT-jártassággal kapcsolatos kvantifikálható adatokat gyűjtöttem. Egyes változókból összetett indexet képeztem. Egyes skála típusú kérdések, az alkalmazott index és szabadszavas mezők kvantifikálása után mindezen adatok tudományos kiértékelése során megállapítottam, hogy a magyar közigazgatásban információbiztonsági tudatosság szempontjából lemaradás tapasztalható. Tézisem alátámasztására felhasználtam a 2013-as Illéssy, Nemeslaki, Som kutatások nyers adatait is, ezeket az eddig nem kiértékelt, nem publikált adatokat újra kiértékeltem, ami szintén alátámasztotta tézisem, és annak pontos megértéséhez nyújtott további információkat.

2) Kutatásom során egy általam kidolgozott újszerű modellt alkalmaztam a közigazgatásra.

Kutatásaim során áttekintettem a vonatkozó nemzetközi és hazai szakirodalmat. Számos modellt és környezeti befolyásoló tényezőt azonosítottam, és azzal kapcsolatos kutatásom vonatkozásában a nemzetközi szakirodalmat áttekintettem. Kitértem a modelleken túl olyan okokra és szervezeti tényezőkre, amelyeket eddig a magyar szakirodalomban nem vizsgált még senki. Ennek során azt tapasztaltam, hogy a magyar szakirodalomban számos modellnek és tudományos vizsgálatnak, megközelítésnek említés szintjén sincs nyoma. Ezen újszerű megközelítések és modellek egybevágtak kutatásaimmal és kialakított oktatásmódszertani megfigyeléseimmel. Ezt az újszerű megközelítést, a feltárt szakirodalomi elméleteket és modelleket alkalmaztam a közigazgatásra a kutatásom során – ilyen alapossággal, ezen modelleket feltárva, megismerve, amelyek a magyar

tudományos szakirodalomban nem vagy elvétve részben voltak meg. Hangsúlyozni kívánom, hogy itt a jelentős és pozitív változást az oktatási modell és módszertan kidolgozása és azon túl annak alkalmazása jelenti, amit és amelynek mérési eredményeit disszertációmban bemutattam.

Kutatásaim, az NKE EIV-ben való oktatás során gyűjtött kutatási kérdőívem révén, a *Safer Internet Programban* és üzleti szférában szerzett oktatási tapasztalataim alapján kidolgoztam az információbiztonsági tudatos viselkedés átültetéséhez egy modellt, a modellem alapján egy mintaelőadást. Valamint részben magyar, részben az interdiszciplináris területeken nemzetközi szakirodalmat dolgoztam fel. A soft, humán tényezők közül viselkedést befolyásoló tényezők, a Theory of Planned Behaviour (TPB, A tervezett viselkedés elmélete), a General Deterrence Theory (GDT, Az általános elrettentés elmélete), a Protection Motivation Theory (PMT, A védelmi motivációs elmélet), a Technology Acceptance Model (TAM, A technológia elfogadási modell) mellett összesen több, mint 54 hasonló elmélet létezik, amely valamilyen módon magyarázza az ember szabálykövetési, szabályalkalmazási hajlandóságát, döntési mechanizmusát. Ide sorolhatóak még egyéb interdiszciplináris tényezőként a tudásmenedzsment, a személyes awareness preferenciák, vagy épp az elrettentési, visszatartási modellek is. A hard, kemény tényezőként a szabályozást vizsgáltam disszertációmban nemzetközi szakirodalmi kitekintéssel. Így voltaképpen a modellem kialakítása során mindkét területen dolgoztam fel nemzetközi szakirodalmat. Ugyanakkor a szakirodalom számos esetben anonimizált szervezetekről és esettanulmányok bemutatásáról szólt, nem volt megállapítható, hogy közigazgatási vagy milyen munkaszervezetről van szó. Általánosságban viszont elmondható, hogy ezek mindegyike számítógépesített munkakörülmények, fehérgalléros munkavállalók bevonásával készült, ahova a közigazgatás is sorolható. Az egyik vállalat esetében, bár rendelkezik gyártókapacitással, azaz olyan munkavállalói is vannak, akik nem vagy jellemzően nem számítógépen dolgoznak, ezen munkaköröket nem érintette a kutatás, mivel abba csak a számítógéppel rendelkező munkavállalók lettek bevonva. Így a hasonló munkakörök, számítógépesített fehérgalléros munkakörök miatt mindenképpen releváns a közigazgatás számára is a kutatási eredményem.

Ezen modell alkalmas lehet arra, hogy jelentősen befolyásolja a szabálykövetési hajlandóságot, és így a gyakorlatba ültesse át a szabályzatban megfogalmazott információbiztonsági alapelveket.

A disszertációmban bemutatott modell alkalmazhatóságát és alkalmazásának eredményeit többezer fős mintán lemértem. Újszerű, nem kizárólag információbiztonsági szempontú, hanem interdiszciplináris megközelítése révén hatékonyabban lehet képes támogatni a tudatossági stratégia, programok, oktatások, tréningek megvalósítását. Olyan eszközöket ad a menedzsment

és az információbiztonsági szakterület kezébe, amelyeket alkalmazva jelentős és pozitív irányú változásokat tudnak elérni. A modell lényege, hogy nem kizárólag a szakmai mondanivalóra koncentrál, hanem az azt körülvevő tényezőket is hasonló súllyal kezeli. Így nem csak a *Miért?* és *Mit?*, hanem a *Hogyan?*, *Kinek?*, *Mikor?*, *Hol?*, *Ki?* és *Mérés* területek is hasonlóan fontosak az eredmény érdekében. A modell magában foglalja, mondhatni garantálja a mérés és visszacsatolás, a ciklikusság miatt a program sikerét, az információbiztonsági képzés fejlődési lehetőségét.

Az ezen modell alapján kidolgozott mintaelőadást nagyságrendileg 4500 fős mintán teszteltem. Ennek eredményei azt mutatják, hogy valóban a jelenléti oktatás hatékony, a szabályalkalmazási gyakorlatban mérhető. Megnőtt a bejelentések száma, tehát a résztvevők tudatosan alkalmazzák az új ismereteket. Viszonylag rövid idő alatt lehet elérni hathatós eredményt; míg e-learning kapcsán ilyen kiugrásokat nem sikerült kimutatni. Elképzelhető, hogy hosszabb távon az is eredményes lehet, bár volumenében nem kecsegtet hasonlóval.

3) Bizonyítottam, hogy oktatással fejleszthető az információbiztonsági tudatossági szint és a szabálykövető magatartás.

Bizonyítottam, hogy az általam kidolgozott modell alkalmazása által az információbiztonsági oktatás segítségével az információbiztonsági előírások ismeretén túl a tudatos és szabálykövető viselkedésben is pozitív változás érhető el. Kiscsoportos oktatás előtt és után elvégzett kérdőíves méréssel ezen mintaelőadást nagyságrendileg 4500 fős mintán teszteltem. Ezen mintán számszerűen kimutatható igazolt hatása volt a felhasználók információbiztonsági tudatossági viselkedésének, hiszen a jelenléti oktatásban résztvevők esetében szignifikánsan megnőtt az információbiztonsági tudatosság, a szabálykövetési hajlandóság; a szabályt a napi gyakorlatban alkalmazták. Az e-learning anyagok kidolgozására is alkalmaztam a modellem; az így publikált anyagokra statisztikai módszerekkel nem volt kimutatható a változás, de a kurzus értékelése, a visszajelzések és a mozgósított létszám tekintetében jelentős áttörés volt.

4) Compliance Check Distance, (CCD) azaz a nemmegfelelőségi gyakorlatból való kockázat kezelésének kidolgozása

A nemmegfelelőségek kezelése lehet előzetes, feltáró, illetve utólagos (preventív, detektív és korrektív tevékenységek). A szabvány alapján egy-egy tanúsítás elvárja, hogy minden évben legyen fejlesztési terület megnevezve. Viszont arra nem térnek ki, hogy amikor mérünk valamit valaminek az érdekében, jó mérési eredmény esetén, ha mindent rendben találnak, akkor miért kéne azt újból vizsgálni, miért kéne rajta változtatni. Ha megvan a jól bevált mérés, gyakorlat, illetve a módszer, akkor miért kellene változtatni? De vajon nem lenne-e szükséges megvizsgálni,

hogy jó dolgot mérünk-e? Elképzelhető, hogy rossz szemszögből, rossz dolgot mérünk, s lehet, hogy az egész folyamat az audit ellenére hibát tartalmaz. Mindezen alattomosan növekvő kockázatok időben történő érzékelésében segíthet az üzleti területről vett, az üzleti folyamatokban már alkalmazott mérési lehetőség. Azokon a területeken, amelyekkel nincs aktív kommunikáció, nincs rendszeres visszacsatolás, még inkább kialakulhatnak olyan folyamatok, amelyeket nem értünk, nem tudunk helyesen mérni, és nem lesznek az információbiztonsági rések feltárva. Ezen nemmegfelelőségek kiküszöbölésére is alkalmas lehet a hármas pontban ismertetett modellem, amely visszacsatolást is tartalmaz éppen ezen okokból. A compliance ilyen módon történő fenntartása ugyanakkor rendkívül költséges lehet, ha ezt minden munkafolyamatra fel kívánjuk írni, a formális logika nyelvén rögzíteni szeretnénk az adott rendszerbe egy munkaszervezetnél. Az általam kidolgozott modell nem képes a teljes GRC terület lefedésére és minden kockázat formalizált felírására, azonban a jelentős eltérések időben történő észlelésére alkalmas lehet, oly módon, hogy a modell révén kapott kimeneti információk a GRC terület, a CCD bemeneti információját képezi, amely így már feltárásra kerül és kezelhető.

6. ÖSSZEGZÉS

Dolgozatom ***központi kérdése*** annak vizsgálata volt, hogy információbiztonsági tudatossági szempontból hol helyezkedik el a közigazgatási szféra, illetve hogyan lehetséges hatékonyan fejleszteni az információbiztonsági szabályalkalmazási hajlandóságot, és milyen módon használható fel az e-learning az információbiztonsági oktatások során.

Az ***információbiztonsági*** szabályalkalmazás, a nemzeti kibertudatossági szint fejlesztéséhez nem elegendőek tisztán információbiztonsági válaszok – összetett problémák megoldásához összetett válaszok szükségesek. A magyar szakirodalomban még nincs elterjedve az interdiszciplináris megközelítés, így a különböző motivációs elméletekre vagy külföldi kutatók által a témában elvégzett mérésekre való hivatkozást ezen a területen nem találtam. Ugyanakkor ezen új területek, ezen elméletek több mint egy évtizede már a kutatók látóterébe kerültek.

A szakirodalom feldolgozása után hipotézisem vizsgálatához kérdőíves felmérést alkalmaztam. Ezen felmérés újszerű módszerek felkutatását és felállítását igényelte. Ezért saját ***modellt*** dolgoztam ki. Ezt a modellt élő oktatások során alkalmaztam, többezer fős mintán vizsgálva hatékonyságát. Valamint a modellt alkalmaztam e-learning megtervezéséhez és létrehozásához. Három ilyen e-learning kurzus esetszámait és eredményeit elemeztem többezer fős mintán.

Az önbevalláson alapuló kérdőívekre adott válaszokat többféle statisztikai módszerrel elemeztem. A kérdőív eredményeit felhasználva feltártam a közigazgatási szféra lemaradását az információbiztonsági tudatosság szempontjából az üzleti szférához képest, amit statisztikai módszerrel is igazoltam.

A kutatások ***eredményeként*** a kérdőíves vizsgálatokat interjús vizsgálatokkal egészítettem ki, valamint tantermi, élő oktatásokat tartottam, e-learning tananyagot készítettem, és mindezeket teszteltem.

A feltételezésem az volt, hogy a jobb szabályértés, a jobb elfogadás, nagyobb szabálykövetési, alkalmazási hajlandóságot feltételez. A kutatásom eredményei ezt alá is támasztották, ennek oka az lehet, hogy az ember kongruens viselkedése élő szituációban, saját élmény megtapasztalása közben könnyebben változtatható.

A vizsgálat alapján fény derült arra is, hogy a jelenléti, élő oktatás a leghatékonyabb. Fontos szerepe lehet ebben az interaktív visszakérdezési lehetőségnek. Aktív csoport esetében, a régóta bent tartott (fel nem tett, megválaszolatlan) kérdések feltevésével egymást támogatják a csoport tagjai. Míg az e-learning képzés esetén nem volt ekkora mértékű változás kimutatható, azonban más tényezők, megfelelő indikátorválasztás mellett lehetséges a középtávú változások vizsgálata,

kimutatása, ha a központi koordináció mellett a mérések és visszajelzések széles közigazgatási körből rendelkezésre állnak. A bevezetett szakszavakra történő későbbi építkezés egy lehetőség, ami jobban befogadhatóvá teszi a szabályalkalmazási gyakorlat további fázisait a megteremtett közös nyelv és alapvetések bevezetését követően.

Az értekezés javaslatai magára az információbiztonsági vezetőképzés alapdilemmájára is segíthetnek legalább részben megoldást találni, azaz, hogy hogyan növelhető a közigazgatási információbiztonsági vezetők vezetői hatékonysága. A vezetői hatékonyságot növelheti, ha a mérési eredmények rendelkezésre állnak; kockázatokkal arányosan a célterületen lehetséges eredményeket elérni. Információbiztonsági vezetőként fel lehet használni azokat a tudományos eredményeket, amelyek megmutatják, hogyan lehetséges szabálykövetési hajlandóságot fejleszteni.

Az értekezés legfőbb újszerűségét szemléletmódja, a szakirodalom nem pusztán információbiztonságról szóló részének hiánypótló elemzése adja, amely kitágítja a szakterület határait. A kezdetben felvetett kutatási problémát maradéktalanul körbejártam, saját modellt állítottam fel, amellyel megvizsgáltam a tárgykört, s végül megválaszoltam a felvetett kérdéseket. Az élő oktatás nagyobb bevonódást, jobb megértést tesz lehetővé, mint a pusztán írásbeli szabályzat elérhetővé tétele. Az e-learning tananyag alkalmas a figyelem felkeltésére és az érintettek bevonására, ugyanakkor szignifikánsan nem befolyásolta a szabálykövetési hajlandóságot. Viszont alacsony költségek mellett, gyorsan, rövid idő alatt lehetséges elérni nagy létszámban a célközönséget. És alkalmas lehet arra, hogy gyorsan és nagy tömegek számára teremtsük meg az alapokat a későbbi fejlesztéshez. Jelentős változások úgy érhetőek el, ha az oktatás erősebb bevonódás, jobb megértés révén nagyobb szabálykövetési hajlandóságot eredményez. Ennek a változását folyamatosan lehetséges mérni megfelelő indikátorokkal. Kidolgozott modellem mind az e-learning, mind az élő oktatásra alkalmazható. A közigazgatásban dolgozó információbiztonsági vezetőket támogatva egy egységes oktatási és mérési módszerrel ez jelentős változásokat hozhat. Jelentős támogatás lehet a közigazgatásban dolgozó információbiztonsági szakembereknek, ha kész modellt tudnak alkalmazni, de még nagyobb, ha ez alapján központilag létrehozott tananyagok állnak rendelkezésre, melyek az adott munkaszervezetekben könnyen megoszthatóak. Valamint ha hasonlóan elérhetőek a képzések előtti és utáni mérésekhez szükséges eszközök, amelyek így közigazgatás szinten válnak transzparenssé, a fejlesztendő területekre irányítva a figyelmet. A központi koordináció növelheti az eredményességet, mivel a mérések és eredmények nagyobb volumenben összehasonlíthatóak és jobban elemezhetőek, mintha szigetszerűen vagy eltérő, nem összevethető mérések állnak rendelkezésre. A jobb megértés és nagyobb szabálykövetési hajlandóság révén mindez a

magánéletben is követendő példaként alkalmazódik majd, így a családtagok, rokonok, ismerősök felé csatornát nyitva a változások átléphetik a szigorúan vett közigazgatási határokat, országos szinten éreztethetik majd hatásukat.

SZAKIRODALOM-JEGYZÉK

ADAMS, A., SASSE, M. A.: Users are not the enemy. - In. Association for Computing Machinery. Communications of the ACM, 1999. 42. sz. - p. 40-87.

AJZEN I.: The Theory of Planned Behavior. - In. Organizational Behavior and Human Decision Processes, 1991. 50. sz. - p. 179-211.

ALBRECHTSEN E.: A qualitative study of users' view on information security. - In. Computer Security, 2007. 26. sz. - p. 276-289.

AL-OMARI, A., EL-GAYAR, O., DEOKAR, A.: Security Policy Compliance: User Acceptance Perspective. System Science (HICSS), The 45th Hawaii International Conference, 2012. - p. 3317-3326.

ANDERSON, C. L., AGARWAL, R.: Practicing Safe Computing: A Multimethod Empirical Examination of Home Computer User Security Behavioral Intentions. - In. MIS Quarterly, 2010. 34. évf. 3. sz. - p. 613-643.

ANDRESS, J., LEARY, M.: Building a Practical Information Security Program. Cambridge, MA: Syngress. 2016, ISBN: 9780128020425. 9780128020883

ARSENIJEVIĆ, O., TRIVAN, D. MILOŠEVIĆ, M.: Storytelling as a modern tool of construction of information security corporate culture. - In. ЕКОНОМИКА, 2016. 62. évf. 4. sz. - p. 105-114.

AU N, NGAI E, CHENG T.: Extending the understanding of end user information systems satisfaction formation: an equitable needs fulfillment model approach. - In. MIS Quarterly, 2008. 32. évf. 1. sz. - p. 43-66.

AYTES K., TERRY C.: Computer security and risky computing practices: A rational choice perspective. - In. Journal of Organizational and End User Computing, 2005. 4. sz. - p. 257-279

AYYAGARI, R., GROVER, V., PURVIS, R.: Technostress: Technological antecedents and implications. - In. MIS Quarterly, 2011. 35. évf. 4. sz. - p. 831-858.

BAGCHI, K., UDO, G.: An analysis of the growth of computer and internet security breaches, - In. Communications of the Association for Information Systems, 2003. 12. évf. 46. sz. - p. 684–700.

BÁNYÁSZ Péter, BÓTA Bettina, CSABA Zágon: A social engineering jelentette veszélyek napjainkban, - In. Biztonság, szolgáltatás, fejlesztés, avagy új irányok a bevételi hatóságok működésében. Magyar Rendészettudományi Társaság Vám- és Pénzügyőri Tagozat, Budapest, - p. 12-37.

BÁNYÁSZ Péter: Kiberbűnözés és közösségi média, - In. Nemzetbiztonsági Szemle, 2017. 5. évf. 4. sz. - p. 12-37.
BARMAN S.: Writing information security policies. New York: New Riders; 2002. 32.o.
BARRA R., MCLEOD A., SAVAGE A., SIMKIN M.: Passwords: do user preferences and website protocols differ from theory? - In. Information Privacy, 2010. 6. évf. 4. sz. - p. 50–69.
BAUER, S., BERNROIDER, E. W. N., CHUDZIKOWSKI, K.: Prevention is better than cure! Designing information security awareness programs to overcome users' non-compliance with information security policies in banks. - In. Computers & Security, 2017. 68. sz. - p. 145-159.
BAYUK J.: How to write an information security policy. In Computerworld 2009. http://www.computerworld.com/article/2525539/security0/how-to-write-an-information-security-policy.html.
BAZERMAN, M.H. TENBRUNSEL, A.E.: Blind Spots: Why We Fail to Do What's Right What to Do About It, Princeton University Press, Princeton, 2011. - p. 216
BEDERNA, ZS., RAJNAI Z., SZÁDECZKY, T.: Business strategy analysis of cybersecurity incidents, Revista Academiei Fortelor Terestre / Land Forces Academy Review, 2021. 26. sz. - p. 139-148.
BEEBE, NL., RAO, VS.: Using situational crime prevention theory to explain the effectiveness of information systems security. Paper presented at the SoftWars conference LasVegas NV; 2005.
BEHRMAN, D., PERREAULT, W. D., Jr.: A role stress model of the performance and satisfaction of industrial salespersons. - In. Journal of Marketing, 1984. 48. évf. 4. sz. - p. 9-21.
BESNARD D, ARIEF B.: Computer security impaired by legitimate users. - In. Computer Security 2004. 23. sz. - p. 253-264.
BEYER M, AHMED S, DOERLEMANN K, ARNELL S, PARKIN S, SASSE A, PASSINGHAM N.: Awareness Is Only the First Step: A Framework for Progressive Engagement of Staff in Cyber Security. Business white paper: Hewlett Packard. 2016.
BODLAKI Ákos, CSERNAY Andor, MÁTYÁS Péter, MUHA Lajos, PAPP György, VADÁSZ Dezső: Miniszterelnöki Hivatal Informatikai Tárcaközi Bizottsága (MeH ITB) 12. számú ajánlása 1996. Informatikai Rendszerek Biztonsági Követelményei, Budapest
BOLLA Marianna, KRÁMLI András: Statisztikai következtetések elmélete, Typotex 2005
BOSS, S., KIRSCH, L., ANGERMEIER, I., SHINGLER, R. AND BOSS, R.: If someone is watching, I'll do what I'm asked: Mandatoriness, control, and information security, - In. European Journal of Information Systems, 2009, 18. évf. 2. sz. - p. 151-164.
BUDAI Balázs Benjámin.: A közigazgatás újragondolása, Akadémiai Kiadó, 2016.
BUDAI Balázs Benjámin: Az e-közigazgatás elmélete, Akadémiai Kiadó, 2016.

BUJDOSÓ Gyöngyi. Meglévő és szükséges informatikai kompetenciák felmérése és kialakítása. - In. Interdiszciplináris pedagógia és a fenntartható fejlődés, 2014. - p. 132–139.

BUJDOSÓ Gyöngyi: Információtranszferhez Szükséges Digitális Írástudás, Digitális Kompetenciák Fejlesztése. - In. Media and E-Learning Environment in Education in V4 Countries, 2015. - p. 132–145.

BULGURCU, B., CAVUSOGLU, H., BENBASAT, I.: Information Security Policy Compliance: An Empirical Study of Rationality-Based Beliefs and Information Security Awareness, - In. MIS Quarterly, 2010. 34. sz. - p. 523-548.

Bundesamt für Sicherheit in der Informationstechnik (BSI)/Federal Office for Information Security. BSI-Standard 100-1. Information Security Management System. Version 1.5. Bonn; 2008. Available from: https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/BSIStandards/standard_100-1_e_pdf.html

BUTHELEZI, M. P., VAN DER POLL, J. A., OCHOLA, E. O.: Ambiguity as a barrier to information security policy compliance: A content analysis. - In. International Conference on Computational Science and Computational Intelligence (CSCI). 2016.

Carmel MCNAUGHT, Paul LAM: Using Wordle as a Supplementary Research Tool, 2010, The Qualitative Report Volume 15. évf. 3. sz. - p. 630-643.

CHAN M., WOON I., KANKANHALLI A.: Perceptions of information security at the workplace: linking information security climate to compliant behavior. - In. International Journal of Information Security and Privacy, 2005. 1. évf. 3. sz. - p. 18-41.

CHAPPLE, C.L. et al.: Social Science Research 2005. 34. sz. - p. 357–383

CHEN CC, MEDLIN BD, SHAW RS.: A cross-cultural investigation of situational information security awareness programs. - In. Information Management & Computer Security. 2008. 16. évf. 4. sz. - p. 360-376

CHEN, Y., RAMAMURTHY, K., & WEN, K.-W.: Impacts of comprehensive information security programs on information security culture. - In. Journal of Computer Information Systems, 2015. 55. évf. 3. sz. 11-19.

CHENG, L., LI, Y., LI, W., HOLM, E., ZHAI, Q.: Understanding the violation of IS security policy in organizations: an integrated model based on social control and deterrence theory. - In. Computers & Security, 2013. 39. sz. - p. 447-459.

CORNELIUS, S., HIGGISON, C.: The Tutor's role. Heriot-Watt University and Robert Gordon University. 2008

COYLE-SHAPIRO JA., KESSLER I.: Contingent and non-contingent working in local government: contrasting psychological contracts. - In. Public Administration, 2002. 80. évf. 1. sz. - p. 77-101.

CRAM, W. A., PROUDFOOT, J. G., & D'ARCY, J.: Organizational information security policies: a review and research framework. - In. European Journal of Information Systems, 2017. 26. évf. 11. sz. - p. 605-641.

CUESTA, L.: The Design and Development of Online Course Materials: Some Features and Recommendations, 2010.

CSÁNYI Vilmos: Az emberi természet Humánetológia évszám, › ** 5. A humán szocialitás ›5.1. A csoportélet (oldalszám? Kell ide?)

CSÁNYI Vilmos: Humánetológia - In. Magyar tudomány 45. évf. 4. sz. 2000. - p. 397-416.

D'ARCY J, HERATH T.: A review and analysis of deterrence theory in the IS security literature: making sense of the disparate findings. - In. European Journal of Information Systems, 2011. 20. évf. 6. sz. - p. 643-658.

D'ARCY J, HOVAV A, GALLETTA D.: User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. - In. Information Systems Research, 2009. 20. évf. 1. sz. - p. 79-98.

DA VEIGA, A. AND MARTINS, N.: Information security culture: a comparative analysis of four assessments, - In Proceedings of the 8th European Conference on IS Management and Evaluation, 2014. 8. sz. - p. 49–57.

DA VEIGA, A.: Comparing the information security culture of employees who had read the information security policy and those who had not, - In. Information & Computer Security, 2016. 24. évf. 2. sz. - p. 139-151

D'ARCY, J., HERATH, T., SHOSS, M. K.: Understanding employee responses to stressful information security requirements: A coping perspective. - In. Journal of Management Information Systems, 2014. 31. évf. 2. sz. 285-318.

DAVENPORT, T. H.: Process Innovation, Harvard Business School Press, Boston, Massachusetts, 1993.

DEÁK Veronika: A közszolgálati kiberbiztonsági képzés lehetősége Magyarországon, Hadmérnök, 2020. 3.szám - p. 157–178.

DHILLON G.: Principles of information systems security. John Wiley & Sons; 2007. http://bvbr.bib-bvb.de:8991/exlibris/aleph/a23_1/apache_media/VAT4XRLXG9LUE9737I4PTM44NIBCA2.p

df Dhillon, Gurpreet, Verfasser Kiadás éve: 2007 Külső leírás: XII, 451 S., Ill., graph. Darst. ISBN:978-0-471-45056-6 0-471-45056-1

DHILLON, G., TORKZADEH, G.: Value-focused assessment of information system security in organizations, - In. Informations Systems Journal, 2006. 16. sz. - p. 293–314.

DINYÁNÉ Szabó Mariann: Tanulásmódszertan, Semmelweis Egyetem, TÁMOP-4.1.2/A/1-11/1-2011-0015 keretében, 2011

DIVER S.: Information security policy: a development guide for large and small companies. <http://www.sans.org> 2007

DOBÁK Miklós, ANTAL Zsuzsa: Vezetés és szervezés. Aula, Budapest, 2010. 42. old. alapján - (Dobák Miklós, Antal Zsuzsa: Vezetés és szervezés Szervezetek kialakítása és működtetése, 10.2.2.)

DOHERTY NF., ANASTASAKIS L., FULFORD H.: The information security policy unpacked: A critical study of the content of university policies. - In. International Journal of Information Management 2009. 29. évf. 6. sz. 449-457.

DUNBAR, R.: Grooming, Gossip and the Evolution of Language. 1996 (London, Faber and Faber).

ELHAM ROSTAMI.: Tailoring policies and involving users in constructing security policies - A mapping study 2019. Conference: HAISA 2019 At: Nicosia, Cyprus

ELLWARDT, L.: Gossip in Organizations. A Social Network Study. (ICS Dissertation Series) Groningen., 2011 https://www.researchgate.net/publication/254821799_Gossip_in_organizations_a_social_network_study

EMINAGAOGLU, M., Erdem UCAR, E., EREN, S.: The positive outcomes of information security awareness training in companies. A case study Information security technical report 14. évf. 2009. - p. 223-229.

Enterprise Strategy Group (ESG). Brief: Cybersecurity Skills Shortage: A State of Emergency. Research Report, IT Spending Intentions Survey; 2016. http://www.esg-global.com]

FLOWERDAY S.V., TUYIKEZE, T.: Information security policy development and implementation: The what, how and who. - In. Computers & Security 2016 61. sz. - p. 169–183

FOGARASSYNÉ Vathy Ágnes, STARKNÉ Werner Ágnes: Intelligens adatelemzés, - Bp. Typotex, 2011

FOSTER, E. K.: Research on Gossip: Taxonomy, Methods, and Future Directions. - In. Review of General Psychology. 2004. 8. évf. 2. sz. - p. 78-99

FURNELL, S.: Assessing password guidance and enforcement on leading websites, - In. Computer Fraud & Security, 2011. 12. sz. - p. 10-18.
FURNELL, S.: Password practices on leading websites - revisited, - In. Computer Fraud & Security, 2014. 12. sz. - p. 5-11.
GALLUCH, P. S., GROVER, V., THATCHER, J. B.: Interrupting the workplace: Examining stressors in an information technology context. - In. Journal of the Association for Information Systems, 2015. 16. évf. 1. sz. - p. 1-47.
GASKÓ Krisztina, HAJDÚ Erzsébet, KÁLMÁN Orsolya, LUKÁCS István, NAHALKA István, PETRINÉ Feyér Judit: A gyakorlati pedagógia néhány alapkérdése Hatékony tanulás. ISBN 963 9704 63 6 ö ISBN 963 9724 04 1, 2006
GAWRON VJ, DRURY CG, FAIRBANKS RJ, BERGER RC.: Medical error and human factors engineering: where are we now? - In. American Journal of Medical Quality, 2006. 21. sz. - p. 57–67.
GOEL, S. SHAWKY, H.A., Estimating the market impact of security breach announcements on firm values, - In: Information & Management, 2009. 46. sz. - p. 404–410.
GOEL, S., CHENGALUR-Smith, I. N.: Metrics for characterizing the form of security policies. - In. The Journal of Strategic Information Systems, 2010. 19. évf. 4. sz. - p. 281-295.
GOEL, S., SHAWKY, H. A.: Estimating the market impact of security breach announcements on firm values, - In. Information & Management, 2009. 46. évf. 7. sz. - p. 404-410.
GOODMAN, S. et al.: Information Security: Policy, Processes, and Practices. Routledge, 2008.
GRÜNING C.: Az eredményes tanulás titka. Garantiert erfolgreich lernen by Christian Grüning, Verlag Grüning, Germany, 2009.
GUO KH , YUAN Y.: The effects of multilevel sanctions on information security violations: a mediating model. - In. Information & Management, 2012. 49. évf. 6. sz. - p- 320–326 .
GUO KH, YUAN Y, ARCHER NP, CONNELLY CE. Understanding nonmalicious security violations in the workplace: a composite behavior model. - In. Journal of Management Information Systems, 2011. 28. évf. 2. sz. - p. 203-236.
HÁMORNIK Balázs Péter, KRASZNAY Csaba: A Team-Level Perspective of Human Factors in Cyber Security: Security Operations Centers, In: Denise, Nicholson (szerk.) Advances in Human Factors in Cybersecurity : Proceedings of the AHFE 2017 International Conference on Human Factors in Cybersecurity, July 17–21, 2017, The Westin Bonaventure Hotel, Los Angeles, California, USA Cham (Németország), Németország : Springer International Publishing, 2017. - p. 224-236.

HANSCHE S.D.: Making security awareness happen. In: Tipton HF, Krause M, editors. Informationsecuritymanagement handbook. 4th ed., vol. 3. NewYork: Auerbach Publications; 2002. - p. 337–351.

HAO C., WENLI L.: Understanding organization employee's information security omission behavior: An integrated model of social norm and deterrence. - In. PACIS 2014 Proceedings.Paper, 2018. 280. sz. https://aisel.aisnet.org/pacis2014/280

HAUCKE A, POKOYSKI D.: Mea culpa - Schuld, Scham und Opferrolle bei Social Engineering. kes. 2018;1:6-8

HEIDRICH Balázs.: Szervezeti kultúra és interkultúrális menedzsment. Human Telex Consulting Kft. 2001.

HERATH T, RAO HR.: Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. - In. Decision Support Systems, 2009. 47. sz. - p. 154-165.

HERATH, T., RAO, H.R.: Protection motivation and deterrence: a framework for security policy compliance in organisations, - In. European Journal of Information Systems, 2009. 18. évf. 2. sz. - p. 106-125.

HIGGINS, G.E., WILSON, A.L. AND FELL, B.D., An Application of Deterrence Theory to Software Piracy, - In. Journal of Criminal Justice and Popular Culture, 2005. 12. sz. - p. 166-184.

HIGGINS: security effectiveness. Int J Inf Manag, 2003. 23. sz. - p. 139-54.

HIRSCHI T.: Causes of delinquency. University of California Press; 1969.

HORVÁTH Dóra, BAUER András: Marketingkommunikáció, Akadémiai Kiadó, 2013.

HORVÁTH Dóra, NYIRŐ Nóra, CSORDÁS Tamás: Médiaismeret Reklámeszközök és reklámhordozók Akadémiai Kiadó, 2016. ISBN: 978 963 05 9724 1 DOI: 10.1556/9789630597241

HORVÁTH Dóra, NYIRŐ Nóra, CSORDÁS Tamás: Médiaismeret Reklámeszközök és reklámhordozók, Akadémia kiadó, 2013.

HU, Q., XU, Z., DINEV, T., LING, H.: Does deterrence work in reducing information security policy abuse by employees? - In. Communications of the ACM, 2011. 54. sz. - p. 54-60.

HWANG, I., CHA, O.: Examining technostress creators and role stress as potential threats to employees. Information security compliance - In. Computers in Human Behavior, 2018. 81. sz. - p. 282-293.

IFINEDO P.: Information systems security policy compliance: an empirical study of the effects of socialisation, influence, and cognition. - In. Information & Management, 2014. 51 évf. 1. sz. - p. 69-79.

IFINEDO P.: Understanding information systems security policy compliance: an integration of the theory of planned behavior and the protection motivation theory. - In. Computers and Security 2011. 31. sz. - p. 83-95.

ILLÉSSY Miklós, NEMESLAKI András, SOM Zoltán: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. - In. Információs társadalom: társadalomtudományi folyóirat, 2014. 14. évf. 1. sz. - p. 52-73.

Információbiztonsági szabványok, egyetemi jegyzet, Szádeczky Tamás, 2014

INGLESANT, P., SASSE, M.A.: The True Cost of Unusable Password Policies Password Use in the Wild, - In. Poceedings of the 28th International Conference on Human Factors in Computing Systems, CHI 2010, Atlanta, Georgia, USA, April 10-15, 2010.

INHO HWANG , OONA CHA: Examining technostress creators and role stress as potential threats to employees' information security compliance - In. Computers in Human Behavior, 81. sz. 2018. - p. 282-293.

ITIL Maturity Model, Axelos Global Best Practice, Axelos Limited 2013.

IVES B, OLSON M, BAROUDI J.: The measurement of user information satisfaction. - In. Communications of the ACM, 1983. 26. évf. 10.sz. - p. 785-793

IZZAT, A.: Cybersecurity Education Based on the NICE Framework: Issues and Challenges. ISACA Journal, 2018, 3. évf. - p. 1–6.

JAI-YEOL SON.: Out of fear or desire? Toward a better understanding of employees' motivation to follow IS security policies, - In. Information & Management, 2011. 48. sz. - p. 296–302.

JAMAL, M.: Relationship of job stress and Type-A behavior to employees' job satisfaction, organizational commitment, psychosomatic health problems, and turnover motivation. - In. Human Relations, 1990. 43. évf. 8. sz. 727-738.

JAMES T, NOTTINGHAM Q, KIM BC.: Determining the antecedents of digital security practices in the general public dimension. - In. Information Technology and Management. 2013.14. évf. 2. sz. - p. 69-89.

Jó állam jelentés 2018, https://joallamjelentes.uni-nke.hu/2018_pages/pdf-serve/non-compress/web_PDF_JAJ_2018.pdf

JOHNSON, M. E., GOETZ, E.: Embedding Information Security into the Organization. - In. IEEE Computer Society, 2007. - p. 16-24.

JOHNSTON A.C., WARKENTIN M.: Fear appeals and information security behaviors: an empirical study. - In. MIS Quarterly, 2010. 34. sz. - p. 549-566.

JOHNSTON, A.C., WARKENTIN, M. & SIPONEN, M. An enhanced fear appeal rhetorical framework: leveraging threats to the human asset through sanctioning rhetoric - In. MIS Quarterly, 2015. 39. évf .1. sz . - p. 113-134.

KAGAN, S.: Kooperatív tanulás. Önkonet, Budapest, 2001.

KAIZER G., CSEH T., VARGA B.: Buzz a magyar kibertérben. HipeRV (a Reklámvonal hipermédia különszáma), 2007. - p. 36-41

KANKANHALLI A, TEO H-H, TAN BCY, WEI K-K.: An integrative study of information systems. Higgins curity effectiveness. - In. International Journal of Information Management, 2003. 23. évf. 2. sz. - p. 139-154.

KEHL, D., Skálák és statisztikák: a méréselméletről és történetéről. Statisztikai Szemle, 2011. 89. évf. 10-11. sz.

KESH, S., RATNASINGAM, P.: A Knowledge Architecture for IT Security. - In. Communications of the ACM, 2007. 50. évf. 7. sz. - p. 103-108.

KFKI Számítástechnikai Rt, verzió 3.1, https://itsmf.hu/documents/itil1attekintes_v3.1.pdf

KJAERLAND M.: A taxonomy and comparison of computer security incidents from the commercial and government sectors. - In. Computers & Security, 2006. 25. sz. - p. 522–538.

KLIEM, R. L.: Risk Management for Business Process Reengineering Projects, Information Systems Management, 2000. 17. évf. - p. 71-73.

KLING R.: Computer abuse and computer crime as organizational activities. - In. Computer/Law Journal, 1980. 2. sz. - p. 186-196.

KNAPPA, K.J., MORRIS, F.R., JR.B, THOMAS E. MARSHALLC, BYRDC, T.A.: Information security policy: An organizational-level process model, - In. Computers & Security, 2009. 48. sz. - p. 493-508.

KOMOR Levente, NAGY Béla: Az emberi tényező jelentősége az informatikai biztonságban (5.5. fejezet). In: Muha Lajos (szerk., 2000): Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig, Verlag Dashöfer Szakkiadó, Budapest.)

KOVÁCS László, KRASZNAY Csaba: Digitális Mohács 2.0: kibertámadások és kibervédelem a szakértők szerint, Nemzet és Biztonság: Biztonságpolitikai Szemle, 2017. 1. sz. - p. 3-16.

KOVÁCS László, KRASZNAY Csaba: Mert övék a hatalom: Az internet politikát (is) befolyásoló hatása a 2016-os amerikai elnökválasztás során STRATÉGIAI VÉDELMI KUTATÓ KÖZPONT (ELEMZÉSEK) / CENTER FOR STRATEGIC AND DEFENSE STUDIES ANALYSES 2017 : 9 pp. 1-11. , 11 p. (2017)

KOVÁCS László: A kibertér védelme, Budapest, Magyarország : Dialóg Campus Kiadó, Nordex Kft. (2018) , 354 p., ISBN: 9786155889639 ISBN: 9786155889646

KOVÁCS László: Európai országok kiberbiztonsági politikáinak és stratégiáinak összehasonlító elemzése, -In. Hadmérnök, 2012. 7. évf. 2. sz. - p. 302 - 311.
Közigazgatási alapvizsga Nyolcadik, az Alaptörvény értékeivel kiegészített kiadás, NKE 2020, A Nemzeti Közszolgálati Egyetem kiadványa
KRAEMER, S., CARAYON, P.: Human errors and violations in computer and information security: the viewpoint of network administrators and security specialists. - In. Applied Ergonomics, 2007. 38. sz. - p. 143–154.
KRASZNAY Csaba, HTE előadás, https://www.hte.hu/documents/10180/4588545/2.4-Krasznay_Csaba.pdf
KRASZNAY Csaba: Információbiztonság vs. Kiberbiztonság, 5. Magyar Jövő Internet Konferencia, Okos város a célkeresztben, 2018. november 28., a Tudomány hónapja keretében
KRAUS L, WECHSUNG I, MÖLLER S.: Psychological needs as motivators for security and privacy actions on smartphones. - In. Journal of Information Security and Applications, 2017. 34. sz. - p. 34-45.
KRUGER H, DREVIN L, STEYN T.: Email security awareness: A practical assessment of employee behaviour. In: Futcher L, Dodge R, editors. Fifth World Conference on Information Security Education. IFIP – International Federation for Information Processing. 237. sz. Boston, MA: Springer; 2007. - p. 33-40.
KSH.hu, Összefoglaló táblák (STADAT), Tájékoztatási adatbázis, Szakstatisztikák témák szerint, kulcsmutatók szerint, Digitális gazdaság és társadalom, 2018, Megjelenés: 2019.12.30.
LÁSZLÓ Gábor: Kockázatértékelés, kockázatmenedzsment, NKE? 2014
LEACH J.: Improving user security behavior. - In. Computers & Security, 2003. 22. évf. 8. sz. - p. 685-692.
LEBEK, B., UFFEN, J., NEUMANN, M., HOHLER,B., BREITNER, M. H.: Information security awareness and behavior: a theory-based literature review, - In. Management Research Review, 2014. 37. évf. 12. sz. - p. 1049-1092.
LEE, Y., LARSEN, K. R. Threat or Coping Appraisal: Determinants of SMB Executives' Decision to Adopt Anti-malware Software, - In. European Journal of Information Systems, 2009. 18. évf. 2. sz. - p. 177-187.
LEVIN, A. (2018). How a security policy could cause the next killer hack. Retrieved from Inc Magazine. https://www.inc.com/adam-levin/how-a-security-policy-could-cause-next-killer-hack.html.

LI H, ZHANG J, SARATHY R.: Understanding compliance with internet use policy from the perspective of rational choice theory. - In. Decision Support Systems, 2010. 48. évf. 4. sz. - p. 635-645.

LU. R., SADIQ, S., GOVERNATORI, G.: Measurement of Compliance Distance in Business Processes, Information Systems Management, 2008. 25 évf. - p. 344-355.

Magyar értelmező kéziszótár, Akadémiai Kiadó, 2014

Magyar szinonimaszótár, Akadémiai Kiadó, 2014,

Magyarország Nemzeti Kiberbiztonsági Stratégiájáról szóló 1139/2013. (III. 21.) Korm. Határozat

MAQOUSI, A., BALIKHINA, T., MACKAY M.: An effective method for information security awareness raising initiative. - In. IJCSIT, 2013. 5. évf. 2. sz. -p. 63-72

MAXION, R. A., REEDER, R. W.: Improving user-interface dependability through mitigation of human error. - In. International Journal of Human Computer Studies, 2005. 63. évf. 1–2. sz. - p. 25–50.

MAYNARD S, RUIGHAVER A, AHMAD A.: Stakeholders in security policy development. In: Proceedings of the 9th Australian Information Security Management Conference. Perth, Western Australia: 2011.

MCLEOD, A., SAVAGE, A., SIMKIN, M.: Passwords: do user preferences and website protocols differ from theory? - In. Information Privacy, 2010. 6. évf. 4. sz. - p. 50-69.

MEYER, J. P., STANLEY, D. J., HERSCOVITCH, L., TOPOLNYTSKY, L.: Affective, continuance, and normative commitment to the organization: A meta-analysis of antecedents, correlates, and consequences. - In. Journal of Vocational Behavior, 2002. 61. évf. 1. sz. - p. 20-52.

MICHELBERGER Pál, – Dombora Sándor: A possible tool for development of information security - SIEM system, - In. EKONOMIKA, 2016. 62. évf. 1. sz. - p. 125-140.

MICHELBERGER Pál: A felhasználói profil szerepe az információbiztonságban, - In. Pro Publico Bono: Magyar Közigazgatás; A Nemzeti Közszolgálati Egyetem Közigazgatás-Tudományi Szakmai Folyóirata, 2015. 3. évf. 4. sz. - p. 34-50

MICHELBERGER Pál: Információ-, folyamat- és vállalatbiztonság, Megjelent: Óbudai Egyetem, Keleti Károly Gazdasági Kar, Budapest, Magyarország 2020, ISBN: 9789634492078

MICHELBERGER Pál: Vállalatbiztonság, -In. Megjelent: Nagy I. Z.. Vállalkozásfejlesztés a XXI. században III.: tanulmánykötet. 2013., - p. 35-52. ISBN:9786155018619

MIKKO S., MIKKO S. M., ADAM M., SEPPO P.: Employees' adherence to information security policies: An exploratory field study, - In. Information & Management 2013. 51. évf. 2.sz.

MIKKO T. SIPONEN.: A conceptual foundation for organizational information security awareness. - In. Information Management & Computer Security, 2000. 8. évf 1. sz. - p. 31-41

Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda, Informatikai Tárcaközi Bizottság ajánlásai, Informatikai biztonsági módszertani kézikönyv, 8. sz. ajánlás, Budapest, 1994

Miniszterelnöki Hivatal, Informatikai Koordinációs Iroda, Informatikai Tárcaközi Bizottság ajánlásai, Informatikai rendszerek biztonsági követelményei, 25. sz. ajánlás, 1.0 verzió, Budapest, 2008

MUHA Lajos, KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, 2004, - p. 13.

MUHA Lajos, KRASZNAY Csaba: Az elektronikus információs rendszerek biztonságának menedzselése, Nemzeti Közszolgálati Egyetem, 2014

MUHA Lajos: A Magyar Köztársaság kritikus információs infrastruktúráinak védelme, PhD értekezés, ZMNE, Budapest, 127 p 2007

MUHA Lajos: Az informatikai biztonság egy lehetséges rendszertana, In: Bolyai Szemle, XVII. évfolyam, 4. szám, Budapest, 2008

MUHA Lajos: Az informatikai biztonság mérése, In: Kadocsa László (szerk.): A Dunaújvárosi Főiskola Közleményei XXXI.: A Magyar Tudomány Napja és a Kreativitás és Innováció Európai Év 2009. tiszteletére rendezett interdiszciplináris tudományos Konferenciasorozat előadásai. Dunaújváros, Magyarország, 2009.11.09 – 2009.11.13.

MUHA Lajos: Kiberhadviselés – kiberbűnözés, In: IDC IT Security Konferencia, Budapest, 2012.03.22

MUHA Lajos: SZÁDECZKY Tamás, Irányítási rendszerek, 2014

NEMESLAKI, A., SASVÁRI, P.: Empirical Analysis of Information Security Awareness in the Business and Public Sectors in Hungary. In Central and Eastern European e|Dem E|Gov Days 2015, Conference Proceedings, pp. 405-418

NIEMIMAA, E., NIEMIMAA, M.: Information systems security policy implementation in practice: From best practices to situated practices. - In. European Journal of Information Systems, 2017. 26. évf. 1. sz. - p. 1–20.

NIEMIMAA, M., LAAKSONEN, A. E., HARNESK, D.: Interpreting information security policy outcomes: A frames of reference perspective. Paper Presented at the System Sciences (HICSS), 2013 46th Hawaii International Conference on System Sciences.

NORMAN, D.A.: Design rules based on analyses of human error. - In. Communications of the ACM, 1983. 26. évf. 4. sz. - p. 254-258.

OLIVER R.: A cognitive model of the antecedents and consequences of satisfaction decisions. - In. Journal of Marketing Research, 1980. 17. évf. 4. sz. - p. 460-469.
PAANANEN, H. , LAPKE, M., SIPONEN, M.: State of the Art in Information Security Policy Development, - In. Computers & Security, 2019. 88. sz. - pp. 14.
PADAYACHEE, K.: A conceptual opportunity-based framework to mitigate the in- sider threat. Paper presented at the Information Security for South Africa, 14-16 Aug. 2013; 2013
PADAYACHEE, K.: Taxonomy of compliant information security behavior. - In. Computers & Security, 2012. 31. évf. 5. sz. - p . 673-680.
PAHNILA S., SIPONEN M., MAHMOOD A.: Employees' behavior towards is security policy compliance. System sciences, 2007. HICSS 20 07. 40th annual Hawaii international conference on IEEE; 2007. 156b-156b.
PAPP, SOM.: A e-befogadás feltételrendszere és annak fejlesztése az információbiztonság tükrében, Doktoranduszok Országos Szövetsége, Publio Kiadó, 2015
PARKER, D. F., DECOTIIS, T. A.: Organizational determinants of job stress. - In. Organizational Behavior & Human Performance, 1983. 32. évf. 2. sz. 160-177.
PARSONS, K., MCCORMAC, A., BUTAVICIUS, M., PATTINSON, M., JERRAM, C.: Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q), - In. Computers & Security, 2013. 42. sz. - p. 165-176.
PERCIO, G., MONTESDIOCA, Z., CARLOS, A., MACADA, G.: Measuring user satisfaction with information security practices, - In. Computers & Security, 2015. 48. sz. - p. 267-280.
PHAM HC., EL-DEN J., RICHARDSON J.: Stress-based security compliance model: an exploratory study. - In. Information and Computer Security, 2016. 24. évf. 4. sz. - p. 326–347.
Platón: Kratülosz 402 A
POEPJES, R., LANE, M.: An Information Security Awareness Capability Model (ISACM)] DOI: 10.4225/75/57b55238cd8d2 Originally published in the Proceedings of the 10th Australian Information Security Management Conference, Novotel Langley Hotel, Perth, Western Australia, 3rd-5th December, 2012
"Ponemon, L. (2017). 2017 Ponemon Institute cost of a data breach study. Forrás: https://securityintelligence.com/media/2017-ponemon-institute-cost-of-a-data-breach-study/ * "
POSTHUMUS S, VON SOLMS R.: A framework for the governance of information security. - In. Computers & Security, 2004. 23. sz. - p. 638-646.
RASMUSSEN, J.: Human errors: a taxonomy for describing human malfunction in industrial installations. - In. Journal of Occupationai Accidents, 4. sz. 1982. - p. 311-333.

REASON, J.: 1990. Human Error. Cambridge University Press, New York.

ROSEMANN, M., MUEHLEN, M.: Integrating Risks in Business Process Models, 16th Australasian Conference on Information Systems, 2005.

ROSENBLUETH A, WIENER N, BIGELOW J.: Behavior, purpose and teleology. - In. Philosophy of Science - In. 1943. 10. évf. 1.sz. - p. 18-24.

ROSKÓ, T., BUJDOSÓ, GY., NOVAC, M.C., NOVAC, O.C.: Enhancing students' privacy awareness: theory and practice on personal data protection through a VR environment, 2021

ROSKÓ, T., SZŐLLŐSI G.J.: Behind passwords: An analysis of preliminary results in order to understand how users protect their privacy, 26. évf. 2021

ROSTAMI E.: Tailoring policies and involving users in constructing security policies -A mapping study. July 2019. Conference: HAISA 2019At: Nicosia, Cyprus

RUIGHAVER AB., MAYNARD SB., CHANG S.: Organizational security culture: extending the end-user perspective. - In. Computers & Security, 2007. 26. évf. 1.sz. 56–62.

SAFA N. S., MAPLE C., WATSON, T., VON SOLMS R.: Motivation and opportunity based model to reduce information security insider threats in organisations. - In. Journal of Information Security and Applications, 2018. 40 . Sz. - p. 247–257.

SAFA N. S., MAPLE, C.: Human errors in the information security realm – and how to fix them (Classification of users' misbehaviour.). 2016. Computer Fraud & Security, 9. sz. - p. 17-20.

SAFA, N. S., MAPLE C., WATSON T., VON SOLMS, R.: Motivation and opportunity based model to reduce information security insider threats in organisations. - In. Journal of Information Security and Applications 40. sz. 2018. - p. 247–257

SAFA, N. S., SOOKHAK, M., VON SOLMS, R., FURNELL, S., GHANI, N. A., HERAWAN, T.: Information security conscious care behaviour formation in organisations. Computers & Security, 2015. 53.sz. - p. 65-78.

SAFA, N. S., VON SOLMS, R., FURNELL, S.: Information security policy compliance model in organizations, Computers & Security, 2016. 56. sz. - p. 70–82

SAFA, N. S., VON SOLMS, R.: An information security knowledge sharing model in organisations. Computers in Human Behavior, 2016. 57.sz. - p. 442-451.

SAFA, N. S., VON SOLMS, R; FURNELL, S.: Information security policy compliance model in organisations. Computers & Security, 2016. 56: p.70-82.

SALANOVA M., GRAU RM., CIFRE E., LLORENS S.: Computer training, frequency of usage and burnout: the moderating role of computer self-efficacy. - In. Computers in Human Behavior 2000. 16. évf. 6. sz. - p. 575-590.

SALMON, K.: Storytelling in Olja Arsenijević: Storytelling as a modern tool of construction of information security corporate culture. 2010.

SAMONASA, S., DHILLON, G., ALMUSHARRAF, A.: Stakeholder perceptions of information security policy: Analyzing personal constructs, - In. International Journal of Information Management, 2020. 50. sz. - p. 144–154

SANS (Security Awareness Report 2017, https://www.sans.org/webcasts/2017-security-awareness-report-104672/

SCHEIN EH. Defining organizational culture. In: Shafritz JM, Ott JS, editors. Classics of organizational theory. 4th ed. New York: Harcourt Brace College Publishers; 1996.

SCHEIN EH.: Coming to a new awareness of organizational culture. In: Kolb DA, Osland JS, Rubin IM, editors. The organizational behavior reader. 1995. 6th ed. Englewood Cliffs, New Jersey: Prentice Hall;

SCHNELL Zsuzsanna: Az elme nyelve. Társalgás és nyelvfejlődés. Akadémiai Kiadó, 2016.

SCHOLL M., FUHRMANN F., SCHOLL LR.: Scientific Knowledge of the Human Side of Information Security as a Basis for Sustainable Trainings in Organizational Practices. In: Proceedings of the 51th Hawaii International Conference on System Sciences (HICSS), Big Island, Hawaii; 2018. pp. 2235-2244. http://hdl.handle.net/10125/50168]

SCHOLL, M.: Information Security Awareness in Public Administrations, Public Management and Administration, Ubaldo Comite, IntechOpen, 2018. DOI: 10.5772/intechopen.74572. Online: https://www.intechopen.com/chapters/59667 *

SHAPPELL, S., DETWILER, C., HOLCOMB, K., HACKWORTH, C., BOQUET, A., WIEGMANN, DA.: Human error and commercial aviation accidents: an analysis using the human factors analysis and classification system. - In. Human Factors: The Journal of the Human Factors and Ergonomics Society, 2007. 49. sz. - p. 227–242.

SHUHAILI T.: Personalising information security education, University of Plymouth, 2014

SIMON HA.: Administrative behavior. 2nd ed. New York: The Free Press; 1957.

SIMONICS István Az információkeresés és feldolgozás eredményeinek vizsgálata, In.: Tóth Péter. Neveléstudományi kutatások a Kárpát-medencei oktatási térben: Pedagogical Research in the Carpathian Basin Educational Space. (2019) ISBN:9788081223105 pp. 91-101 vagy : https://ppk.elte.hu/file/simonics_istvan_phd.pdf doktori *

SINGH, AN., PICOT, A., KRANZ, J., CUPTA, M.P., OJHA, A.: Information security management (ism) practices: Lessons from select cases from India and Germany. - In. Global Journal of Flexible Systems Management. 2013. 14. sz. - p. 225-239.

SIPONEN M., PAHNILA S., MAHMOOD A.: Employees' Adherence to Information Security Policies: An Empirical Study, In: VENTER H., ELOFF M., LABUSCHAGNE L., ELOFF J., VON SOLMS R. (eds) New Approaches for Security, Privacy and Trust in Complex Environments. SEC 2007. IFIP International Federation for Information Processing, vol 232. Springer, Boston, MA. https://doi.org/10.1007/978-0-387-72367-9_12

SIPONEN, M., VANCE, A.: Neutralization: new insights into the problem of employee systems security policy violations. - In. MIS Quarterly, 2010. 34. évf. 3. sz. - p. 487-502.

SOM Zoltán, ERDŐSI Péter Máté, PAPP Gergely Zoltán, PÓLYA Balázs: Információbiztonsági pillanatkép és helyzetértékelés a magyar közigazgatásban, Óbudai Egyetem, A 6. Báthory-Brassai Nemzetközi Multidiszciplináris Konferencia, 2015. *

SOM Zoltán, PAPP Gergely: Hungarian Trends in Password Usage, in an International Comparison - In. Central and Eastern European eGov Days, 2015. - p. 294-314.

SOM Zoltán: Biztonság támogatása, egyetemi jegyzet, NKE, 2014, ISBN:978-615-5057-54-0

SOM Zoltán: Információbiztonsági alapok és jelszóhasználati statisztikák. A jelszó, a bizalom és az e-befogadás összefüggései napjainkban, - In. Hírvillám, 4, VII. évf, 1. szám, - p. 47-59.

SOM Zoltán: Kockázatmenedzsment gyakorlat, egyetemi jegyzet, NKE, 2014, ISBN: 978-615-5057-55-7

SPEARS J, BARKI H.: User participation in information systems security risk management. - In. MIS Quarterly, 2010. 34. évf 3.sz - p. 503-522.

STANTON J, MASTRANGELO P, STAM K, JOLTON J.: Behavioral information security: two end user survey studies of motivation and security practices. In: Proceedings of the 10th Americas conference on information systems; 2004. p. 1-7.

STANTON J., STAM, K., MASTRANGELO, P., JOLTON, J.: Analysis of end user security behaviors, - In. Computers and Security, 2005. 24. évf. 2. sz. - p. 124–133.

STEVENS, S. S.: On the Theory of Scales of Measurement. American Association for the Advancement of Science. 1946, 103. évf. 2684. sz. pp. 677–680.

STOKES, J.: 2000. Stock Watch. Denver Rocky Mountain News, 2000.

STRAUB D. W., GOODMAN S., BASKERVILLE L. R.: Information Security: Policy, Processes, and Practices. M.E. Sharpe, Inc. Armonk, NY: Routledge, 2008. ISBN 9780765617187.

STRAUB D.W., NANCE W.D.: Discovering and disciplining computer abuse in organizations: a field study. - In. MIS Quarterly, 1990. 14. évf. 1. sz. - p. 45-60.

STRAUB D.W., WELKE R.J.: Coping with systems risk: security planning models for management decision making. - In. MIS Quarterly, 1998. 22. évf. 4.sz. - p. 441-469.

STRAUB, D.W.: Effective IS Security: An Empirical Stud, - In. Information Systems Research, 1990. 1. évf. 3. sz. - p. 255-276.

SVERKE, M., GALLAGHER, D., HELLGREN, J.: In: Health effects of the new labor market (pp.). Alternative work arrangements: Job stress, well-being, and work attitudes among employees with different employment contracts Isaksson (ed.). USA: Kluwer; 2005 .

SZÁDECZKY Tamás, Az IT biztonság szabályozása, Berlin, Németország : GlobeEdit (2018) , 319 p., Kiadónál ISBN: 9786202487641 Amazon REAL ResearchGate publ.

SZÁSZ Antónia, KISS Gábor, Jelszóvisszafejtő programok oktatási célú felhasználása és hatásuk az információbiztonsági tudatosságra, - In. Információs Társadalom, 2018. 18. évf. 3–4. sz - p. 82–104.

SZUBA T.: Safeguarding your technology: practical guidelines forelectronic education information security. <http://nces.ed.gov/pubs98/98297.pdf> 1998, U.S. Department of Education

TALBOT S,WOODWARD A.: Improving an organisations existing information technology policy to increase security. In: Proceedings of the 7th Australian Information Security Management Conference. Perth,Western Australia: 2009.]

TARAFDAR, M., TU, Q., RAGU-NATHAN, B. S., RAGU-NATHAN, T. S.: The impact of technostress on role stress and productivity. - In. Journal of Management Information Systems, 2007. 24. évf. 1. sz. - p. 301-328

TARJÁN Gábor: Az információbiztonsági tudatosság érettségi szintjének mérése szervezetekben, 2020

TARJÁN Gábor: Vezetéstudomány, 2018, https://journals.lib.uni-corvinus.hu/index.php/vezetestudomany/article/view/138

THOMSON, K. VAN NIEKERK, J.: Combating information security apathy by encouraging prosocial organisational behaviour, - In. Information Management & Computer Security, 2012. 20. évf. 1. sz. - p. 39-46.

TIHANYI, N.: Comparison of Two Hungarian Password Databases, - In. Pollack Periodica, 2013. 8. évf. 2. sz. - p. 179–186.

TÖRLEY Gábor: Informatikai biztonságtudatosság, ELTE Informatikai Kar, 2019, ISBN 978-963-489-148-2

TÖRLEY Gábor: The Level of Information Security Awareness of First-Year University Students, 2020, In: The 11th International Conference on Applied Informatics, 2020.01.29-2020.01.31, Eger.

TURKANOVI M, POLAN CIC G.: On the security of certain e-communication types: risks, user awareness and recommendations. - In. Journal of Information Security and Applications, 2013. 18. sz. - p. 193-205.

TYLER, T.R., BLADER, S.L.: Can businesses effectively regulate employee conduct? The antecedents of rule following in work settings. -In. Academy of Management Journal 2005. 8. évf. 6. sz. - p. 1143–1158.

VACZI, D. TOTH-LAUFER, E. SZADECZKY, T.: "Fuzzy-based Cybersecurity Risk Analysis of the Human Factor from the Perspective of Classified Information Leakage," 2020 IEEE 18th International Symposium on Intelligent Systems and Informatics (SISY), 2020, pp. 000113-000118, doi: 10.1109/SISY50555.2020.9217053.

VAKOLA, M., NIKOLAOU, I.: Attitudes towards organizational change: What is the role of employees' stress and commitment? -In. Employee Relations, 2005. 27. évf. 2. sz. - p. 160-174.

VANCE, A., SIPONEN, M., PAHNILA, S.: Motivating IS security compliance: Insights from Habit and Protection Motivation Theory, -In. Information & Management 2012. 49.évf. 190-198.

VANCE, A., SIPONEN, M.: Is security policy violations: a rational choice perspective. -In. Journal of Organizational and End User Computing, 2012. 24. évf. 1. sz. - p. 21-41

VERTON, D.: The Hacker Diaries. New York: McGraw-Hill, Inc.; 2002

VON SOLMS R.,THOMSON K-L, MANINJWA P.: Information security governance control through comprehensive policy architectures. Proceedings of the 2011 - In Information Security for South Africa, 2011.

VON SOLMS S.H.:The 5 Waves of Information Security: From Kristian Beckman to the Present. In: Rannenberg K, Varadharajan V, Weber C, editors. SEC 2010, IFIP International Federation for Information Processing AICT 330. 2010;1-8

WARKENTIN, M., WILSON, R.: Behavioral and policy issues in information systems security: the insider threat, - In. European Journal of Information Systems, 2009. 8. sz. - p. 101–105.

WHITMAN ME.: Security policy: from design to maintenance. In: Straub DW, Goodman S, Baskerville RL, editors. Information security: policy, processes, and practices. - In. Advances in management information systems, Armonk, N.Y.: M.E. Sharpe; 2008. 11. sz. - p. 123–151.

WHITMAN, M. E., MATTORD, H. J.: Principles of Information Security (Second Edition). 2005. Boston: Thomson Course Technology.

WHITMAN, M.E., MATTORD, H.J.: Management of Information Security. Thomson Course Technology, Boston, MA, 2004.

WOODWARD, T.S.: Improving an organisations existing information technology policy to increase security. In: Proceedings of the 7th Australian Information Security Management Conference. Perth, Western Australia, 2009.

WOON I. M. Y, TAN, G. W., LOW, R. T.: A Protection Motivation Theory Approach to Home Wireless Security, Proceedings of the Twenty-Sixth International Conference on Information Systems, Las Vegas, 2005, 367-380.

WORKMAN M.: Gaining access with social engineering: An empirical study of the threat. -In. Information Systems Security. 2007. 16. évf. 6. sz. - p. 315-331

ZEIGARNIK, B.: On finished and unfinished tasks, Psychologische Forschung, 1927. 9. sz.

MELLÉKLETEK

1-5. SZÁMÚ MELLÉKLETEK, KÉRDŐÍVEK, INTERJÚKÉRDÉSEK

1. Illessy_Nemeslaki_Som_kerdoiv.pdf (1. sz. m.)
2. Jelszóhasználati szokások megismerése.pdf (2. sz. m.)
3. NKE_EIV_kerdesek.xlsx (3. sz. m.)
4. eloadas_elott.xlsx (4. sz. m.)
5. eloadas_utan.xlsx (5. sz. m.)

6-11. SZÁMÚ MELLÉKLETEK, STATISZTIKAI ELEMZÉSEK ÉS TÁBLÁZATOK

6. 6.sz.melleklet_stat_probak_H1.xlsx (6. sz. m.)
7. 7.sz.melleklet_stat_probak_H2.xlsx (7. sz. m.)
8. 8.sz.statisztikai_probak_2_melleklet_T2-Acomp.xlsx (8. sz. m.)
9. 9.sz. melleklet_statisztikai_probak_T2-Kolm-Acomp.xlsx (9. sz. m.)
10. 10.sz.melleklet_statisztikai_probak_T3-Bcomp.xlsx (10. sz. m.)
11. 11.sz.melleklet_statisztikai_probak_T3-Bcomp-statprobak.xlsx (11. sz. m.)

12. SZÁMÚ MELLÉKLET, RÖVIDÍTÉSEK JEGYZÉKE

NKE: Nemzeti Közszolgálati Egyetem

EIV: Elektronikus információbiztonsági vezető szakirányú továbbképzési szak

As-Is állapot: jelen állapot, az aktuális állapot leírására használt kifejezés

Dezinformációs, fakenews: olyan hírek, híroldalak, pletykák, hírdetések melyeknek a megtévesztés, félelemkeltés, vagy egyéb hátsó szándékkal készülnek.

BYOD: (bring your own device) Hozza magával saját készülékét vagy más néven hozza magával a saját technológiáját, hozza magával a saját telefonját és hozza magával a személyi számítógépét. Ez a kifejezés azt jelenti, hogy megengedett a saját (munkavállalói) tulajdonú eszköz használata, ahelyett, hogy hivatalosan biztosított készüléket használnának.

MDM: Mobile Device Management, A mobileszköz-kezelés a mobileszközök, például okostelefonok, laptopok adminisztrációját jelenti, voltaképpen egy felügyeleti funkciót lát el tipikusan hordozható eszközökön.

IBSZ: Információbiztonsági Szabályzat. Ennek megnevezése munkaszervezetenként változhat, Informatikai biztonsági szabályzat, utasítás is lehet.

IBF: Az Információbiztonsági Felelős vagy vezető személy rövidítése.

LMS: Learning management system, tanulás kezelő, támogató rendszer.

SCORM: Sharable Content Object Reference Model, megosztható tartalmi objektumok hivatkozási modelljét értjük alatta. Tetszőleges fájl típusok rendszerezését, tananyaggá alakítását értjük alatta.

Moodle: nyílt forráskódú e-learning rendszer.

ISACA: Information Systems Audit and Control Association

CISA, CISM, CRISC, CGEIT: Certified Information Systems Auditor , Certified Information Security Manager, Certified in Risk and Information Systems Control, Certified in the Governance of Enterprise (forrás: https://engage.isaca.org/budapestchapter/minositeseink)

ENISA: Európai Uniós Hálózat- és Információbiztonság

13. SZÁMÚ MELLÉKLET, TÁBLÁZATJEGYZÉK

14. SZÁMÚ MELLÉKLET, ÁBRAJEGYZÉK

15. SZÁMÚ MELLÉKLET, ELÉGEDETTSÉG ÉS MOTIVÁCIÓ

Aytes és Connolly (2004) a biztonságos viselkedés elfogadásának szándékát racionális választásnak tekintette, amely a biztonsági gyakorlatok használhatóságának egyéni megítélésén és az ilyen gyakorlatok elmaradásának következményein alapul. A felhasználók egymással összekapcsolódó szervezeti, technológiai és egyéni tényezők révén alakítják ki az információbiztonsággal kapcsolatos attitűdöket. Ezek a tényezők befolyásolják a felhasználói viselkedést, befolyásolják az információbiztonsági gyakorlatokkal való munka motivációit, összeférhetetlenséget okoznak az információs rendszer működése és az információbiztonsági gyakorlatok között, valamint befolyásolják a dokumentáció , szabályzatok és a figyelemfelkeltő kampányok hatását a biztonsági viselkedésre Albrechtsen (2007) alapján.

A felhasználói (információbiztonsági szempontú) elégedettség mérése az információbiztonsági gyakorlatokkal kapcsolatosan megfelelő kiindulópont lehet a felhasználók viselkedésének diagnosztizálásához. Ezáltal metrikákat biztosítva a menedzsment számára az információbiztonsági képzési és tudatossági programba történő befektetés értékelésére (ROI).

A társadalmi szabályok és a munkahelyi interakciók befolyásolják az egyén információbiztonsági megértését (Albrechtsen, 2007). Tehát a szabályok megértése nagyban befolyásolhatja azok követésére, betartására való hajlandóságot. Modellben részben erre fókuszálok, amelynél a megértés természetesen nem és nem is lehet bit szintű, de látja és megtapasztalja, ahogy a fentiekben ennek matematikai alátámasztásáról már írtam.

A felhasználók információbiztonsági figyelme személyes és szervezeti tényezők kombinációjával függ össze, például elégedettség a támogató szolgáltatásokkal, az elégedettség a fizetéssel, az elégedettség a kollégákkal, a szervezeti elkötelezettség, a technikai ismeretek és érzelmi események Stanton et al. (2004) szerint. Annak megértése tehát, hogy az egyes akadályozó tényezők miért szükségesek, (az önigazolás fontossága) rendkívül fontos. Csakúgy, mint az, hogy az adott feladat hogyan végezhető el szabályosan, (szabályszegés nélkül) milyen megoldásokat kínál a szervezet a feladat teljesíthetőségére. Ismert-e a probléma (hivatalosan nem teljesíthető feladat) a vezetőség vagy az információbiztonsági szakterület előtt.

A felhasználói elégedettség az a mérték, amikor a felhasználó úgy gondolja, hogy a rendszer kielégíti információigényét, ami azt sugallja, hogy a felhasználói igényeket kielégítő információs rendszerek megerősítik elégedettségüket Ives et al. (1983), Au és mtsai. (2008) a felhasználói elégedettséget úgy definiálta, mint azt az affektív és kognitív értékelést, amelyet a felhasználó egy információs rendszer használatával egy kellemes tapasztalatból fejleszt ki.

Oliver (1980) kidolgozta az elvárásmegerősítés elméletét, amely a megerősítés paradigmáját használja az elégedettség értékelésére. Ez az elmélet azt sugallja, hogy az elvárás olyan referenciakeretet hoz létre, amelyben az egyén összehasonlító ítéletet mond a termék teljesítményéről. A vártnál rosszabb teljesítmény ebben a referenciakeretben „alul" van besorolva, ami negatív megerősítéshez vezet. A vártnál jobb teljesítmény ebben a referenciakeretben „fent" -nek minősül, ami pozitív megerősítést generál. Az elvárás és a teljesítményváltozók tehát befolyásolják a felhasználói elégedettséget (Oliver, 1980).

A felhasználók elégedetlensége a biztonsági gyakorlatokkal (el nem fogadásával kapcsolatban) kockázatot jelenthet az információs rendszerek védelmére, és végső soron biztonsági fenyegetést jelent a szervezetek számára. Ennek a negatív kapcsolatnak, a megváltoztatásának egyik módja lehet a felhasználók részvétele a biztonsági gyakorlatok kidolgozásában. Spears és Barki (2010) megerősítették, hogy a felhasználói részvétel az információbiztonsági kockázatok kezelésében az egyik módja a biztonsági problémák elkerülésének. A következetes szabályzatok kidolgozása, a felhasználói és szervezeti igények kombinálása, valamint az információs rendszerekkel interakcióba lépő emberek hatékony bevonása ösztönözheti a biztonsági magatartás elfogadását Johnston és Warkentin (2010). Amely voltaképpen összecseng azzal a megközelítéssel, hogy a szabályok ismerete,megértése, elfogadása növeli annak elfogadását, betartására való hajlandóságot.

Miért fontos, hogy mérjük és tisztában legyünk a felhasználói visszajelzésekkel, elégedettségi tényezőkkel? Hiszem, az egyik nézőpont, hogy a kiadott szabályzatokat be kell tartani, ez különösebb kommentárt (támogatást) egyéb komponenst nem igényel. Másrészről azonban fel kell vetni a kérdést, hogy vajon melyik szabályt, utasítást, elvet könnyebb betartani, követni; amellyel egyet értünk, vagy amelyikkel nem. Egyszerű lenne a válasz, de tovább kell vizsgálni, árnyalni ezt a kérdést. Ugyanis nem pontos a kérdésfeltevés. Nem az a pontos kérdés, hogy egyetértenek-e vele vagy sem, hanem, hogy egyáltalán felfogja, megértik e az emberek a szabályokat, a szabályok okát, annak kockázatcsökkentési stratégiáját. Megérti-e, hogyan kell végrehajtani, hogyan kell alkalmazni azt a szabályt a saját munkafolyamatában. Képes-e, tudja-e alkalmazni önerőből az előírást.
Nézzünk erre egy példát, egyszerű utasítás, hogy például jelzőlámpa nélküli kereszteződésen mielőbb átmegyünk, nézzünk körül. Gyerekeknek sokat mondogatjuk, aztán jó esetben ez a hétköznapi rutin része lesz. A szabály felfogható, érthető, hogy elkerüljünk egy nagy sebességgel haladó gépjárművet, vonatot, vagy éppen biciklit, bármilyen ütközést. Az információbiztonság

szabályai nem mindig ennyire transzparensek. És bár a keménykalapos információbiztonsági szabályzatot képviselő irányvonal azt mondhatja, hogy nem szükséges a szabály mélyebb értelmezése, indoklása, elegendő annak ismerete, betartása. Ugyanakkor van ezzel egy nagyon komoly bökkenő, ellenérv. Mivel nem adható az élet minden területére, teljességére, így annak részhalmazára sem a munkahelyi viselkedésre, szabályokra sem teljeskörű és minden területet, minden mozzanatot lefedő ajánlás, szabály, így az nem is lesz ennek az elvárásnak megfelelő. Tehát nem lehetséges olyan szabályzatot írni, amely az adott munkaszervezet, minden egyes szerepkörére, annak minden egyes munkafolyamatára, adatkezelési folyamatára, információs rendszereire, stb. teljes részletességgel leírja a helyes és helytelen gyakorlatokat, összességében az elvárásokat.
Ezért szükséges a szabályzat (kiváltó, értelmi) okainak áttekintő ismerete, hogy egy kicsit más értelmezésben, körülmények esetén is megvalósulhasson a szabálykövetés. Az elejére visszacsatolva tehát az értelmetlennek tűnő, akadályozó szabályok követése sokkal alacsonyabb lehet, míg a közepes, vagy mélyebb értelemmel és megértéssel felruházott szabályok vagy irányelvek esetén. Ezért fontos képesnek lenni a visszajelzések érzékelésére és fogadására és támogatást nyújtani a ezen megkeresésekre, sőt kommunikációs szempontból roppant fontos ezen megkeresések megköszönése, a pozitív visszacsatolás is.

Ezek alapján kirajzolódik, hogy miért fontos megértenünk a motiváció szerepét az információbiztonsági oktatások vagy információbiztonsági szabálykövetés tekintetében. Bár a kérdést, csak szűken az információbiztonsági terület határáig, az pszichológia területére csak a szükséges mértékben áttérve vizsgálom, mégis látható, hogy rendkívüli jelentősége van. Hiszen annak megértése, hogy mi motiválja a közigazgatási munkavállalókat az információbiztonsági szabályzat megismerésére, szabálykövetésre, a megismert elvárások betartására, a tudatos és proaktív viselkedésre, hozzájárulhat ahhoz, hogy mindezen tevékenységeket a kevésbé szabálykövető munkavállalókra is jobban ki lehessen terjeszteni.

Továbbá és tekintettel az emberek jelentős szerepére a biztonság irányításában, indokolja ennek mélyebb vizsgálatát. Eredeti kérdésem átfogalmazva így is feltehető: Miként lehet motiválni az alkalmazottakat a szervezet biztonsági teljesítményének javítására.
Habár számos olyan elmélet van, hogy az elrettentés elméletétől (general deterrence theory, GDT) függő külső motivációs modellben gyökerezik, azonban a belső motivációs modellt is figyelembe kell venni, hogy segítsen megérteni, hogy az alkalmazottak miért követik vagy nem tartják be a szervezet biztonsági szabályait. Ugyanakkor a Son (2011) szerint , a belső motivációs modellben

gyökerező megközelítéssel jobban meg lehet magyarázni az alkalmazottak biztonságával kapcsolatos szabálykövető magatartását. Son az alkalmazottak motivációjának modelljét az információbiztonsági szabályzatnak való megfelelés érdekében vizsgálja, beleértve, vizsgálva az emberi viselkedés külső és belső modelljeit egyaránt, vizsgálatát 602 személyen végezte el. Kimutatta, hogy az intrinsic (belső, belülről fakadó) motivációs modellben gyökerező változók lényegesen jobban járultak hozzá a munkavállalók megfelelésének magyarázott változatosságához, mint azok, amelyek az extrinsic (külső) motivációs modellben gyökereztek.
A biztonsági események sajátossága, hogy meglepő módon sok eseményt a szervezeti tagok (munkavállalók vagy más módon foglalkoztatottak) követnek el (a tűzfalon, vagy valamilyen védelmi vonalon belül). Goel és Shawky (2009) Ebben az értelemben és ebben a megközelítésben a munkavállalók minden szinten a leggyengébb láncszemek az információbiztonságban. Azaz ahogy az már megállapításra került, nincs tökéletes biztonság, a legmodernebb védelmi rendszerek sem képesek a felhasználói hibák, az összes lehetséges hibalehetőség megakadályozására, megelőzésére, vagy éppen a hanyagságból netalántán a szándékos visszaélések kivédésére.

Warkentin és Wilson (2009) szerint az alkalmazottak fenyegetést jelenthetnek, akár szándékosan, mert bevonódhatnak szándékos visszaélésbe (pl. adatlopás, adatmegsemmisítés, adat szivárogtatás stb.) Vagy nem szándékos vagy véletlen eseményekbe (például a jelszó megváltoztatásának elfelejtése, a kijelentkezés elfelejtése stb.) események kezelésének, vagy jelentés elmulasztásának hibájába eshetnek. Mivel a munkavállalók vagy más módon foglalkoztatottak (és számos beszállító, külső partner is) közvetlen hozzáféréssel rendelkeznek a szervezet hálózatához, így gyakran azoknak a tolvajoknak vagy hackereknek a célpontjává válnak, akik social enginering, vagy hacker technikákkal próbálnak hozzáférni, hozzáférést szerezni a szervezet információihoz, hálózatához.
Elsődleges cél, hogy átvinni valamilyen gondolatot, amely ma és a későbbiekben képes befolyásolni az egyén döntéshozatali folyamatait. Ezeket ritkán lehet direkt állításokkal átvinni. Mivel véleményem szerint szerint azok nem serkentenek gondolkodásra. Így ennél jobb megoldás lehet, -saját oktatói több száz órás előadói meglátásom szerint, a kérdésekkel operálni, kérdéseket feltenni. Ez pedig kombinálva a saját élménnyel, ebből is s legerősebb a helyszíni átélés. Ennek a gondolatnak az átvitele lehet egy-egy előadás, egy - egy oktatási impulzusnak a célja. Mivel az is belátható, hogy nem lehetséges egyszerre, minden információbiztonsági területre kiterjedő szabályzat átvitele, oktatása. Ezért fogalmazódik meg disszertációmban is a szerepkör alapú oktatások fontossága. Hiszen, ha valaki A szerepkörben dolgozik, akkor számára az (felmérés és

kockázatértékelés alapján) ahhoz a szerepkörhöz rendelt, oktatások és információk, szabályok elsajáítása és betartása a legfontosabb (elvárás.) Míg, ha valamely másik személy Z szerepkörben (felmérés eredményeképpen) részben, vagy teljesen más kockázatokat jelent, akkor részben vagy egészen más oktatásokra és szabályokra tevődik a fókusz. Rövid példát bemutatva, egy fizikai védelmi kontrollokban részt vevő portás, vagy biztonsági őr egészen más területre és kockázatokra kell, hogy fókuszáljon, mint mondjuk egy információbiztonsági üzemeltető aki a tűzfalat, vagy egyéb védelmi rendszereket üzemeltet, vagy az információs rendszer üzemeltető, aki a sérülékenységekre kiadott biztonsági frissítést telepíti. Ezen kívül a közigazgatás teljes vertikumát tekintve (Rendőrség, NATO tagságból fakadó ellátandó feladatok, fejlesztő mérnökök, stb.) egészen speciális szerepkörök is lehetnek.

Meglátásom szerint a kapcsolódási pontokat nem találó információk (információ áradat) pl.: olvasd végig a 100 oldalas biztonsági szabályzatot, amelyből csak számodra, a A, K, Z szerepkörre csak 3x5 oldalnyi rész a releváns, roppant kontraproduktív, ellenállást vált ki. Ezen túlmenően az egyén sok esetben nem lesz képes a számára lényeges információkat megtalálni a teljes anyagban, információ áradatban. A túl sok nem releváns információ feldolgozása során feladhatja.

Saját oktatási tapasztalataim alapján, amely során több ezer személy tekintette meg előadásaimat, megfigyeltem, hogy a saját megtapasztalás, a saját élethez és gondolatokhoz nyújtott kapcsolódási pontok lehetnek a legeredményesebbek, a beépülés, gyakorlatba való átültetés, alkalmazás szempontjából. Saját és élményalapú tanulás. Végső soron, bár a GDT-t hatékony stratégiának nevezték, vagy akként használnák, amely megakadályozza, hogy a munkavállalók visszaéljenek szervezeteik információs eszközeivel. Ennek az elméleti megoldásnak a hatékonyságát azonban többen megkérdőjelezték, mert a tanulmányok vegyes eredményeket közöltek azok hatásairól, mint a munkavállalók magatartásának hatékony szabályozóiról. Ezek a megfontolások és tanulmányok, amelyek a munkavállaló viselkedését a munkaszervezeti magatartását vizsgálják az emberi motiváció szociálpszichológiai szakirodalmából származnak. És gyakran magyarázták az alkalmazottak szabálykövető magatartását az emberi viselkedés két motivációs modelljével T.R. Tyler, S.L. Blader, (2005) az egyik egy külső motivációs modell (az észlelt következményekre összpontosítva, mint pl. büntetés vagy jutalom, a szabályok megsértése esetén), a másik pedig egy belső motivációs modell (a szabályok betartása, követése, mert az alkalmazottak a szabályokat betartó vágyuk miatt tartják be a szabályokat). Itt fontos megemlíteni a dolgozatban már részletesen kifejtett elméletemre való hivatkozást, miszerint senkit sem lehet meggyőzni, saját belső koherens világához illeszti mindig az új információkat. Épp ezért a cél sokkal inkább olyan új és befogadható információk adása, amelyek a helyes döntéshozatalban képesek a

munkavállalókat támogatni. A szakirodalom jelentős része ezért a GDT-t elveti. Velemenyem szerint is a transzparens szankció ismeretése bár fontos és ahogy fentebb már kifejtettem annak gyorsasága, stb. releváns lehet a hatás szempontjából, nagysága azonban kevésbé mutat használható eszközt az információbiztonsági szakterület kezében.

A munkavállalói szabálykövető szakirodalomban tehát erős empirikus bizonyítékok állnak rendelkezésre arról, hogy a munkavállalók felfogása az értékek kongruenciájáról a munkáltatójukkal növeli annak valószínűségét, hogy betartják a munkáltató által bevezetett szabályokat. A szankciók megléte és kommunikációja, gyorsasága gyengébb összefüggést mutat, míg a szankció nagysága még alacsonyabbat.
Chan M, Woon I, Kankanhalli (2005) alátámasztja, hogy a belső kongruencia, a munkaszervezet iránti elhivatottság, a munkatársakkal, vezetővel való kapcsolat, stb. nagyban, jelentősebben meghatározza, befolyásolja a szabályzat követési hajlandóságot, mint a külső tényezők, pl.: büntetés, szankciók, elrettentés.

Ugyanakkor amennyiben nemzetgazdasági érdekeket tekintünk, akkor nem lehet kevesebb a cél, mint, hogy az egyik legjelentősebb munkáltatói, (az állam) a közigazgatási információbiztonsági tudatossági szint emelése révén nemzeti hatást érhessen el. Fontos azonban kihangsúlyozni, hogy a pontos és teljes (nemzeti, közigazgatási) mérés nélkül ez nem tekinthető egyedüli üdvözítő, helyes és teljes megoldásnak. Ennek oka, hogy más-más szoció – közösségeknél (életkor, csoportnyomás, IKT tudás, munkaszevezeti elköteleződés, vezetői példamutatás, stb. egyéb változó környezeti tényezők nagyban, jelentősen befolyásolhatják a szabálykövetési hajlandóságot, vagy épp az adott terület, az adott oktatás, annak kulcsüzenetének a megértését.
Mindezekből, a nemzetközi szakirodalom áttekintésből következik, hogy véleményem szerint a magyar szakirodalomból, hiányzott az alkalmazottak információbiztonsági megfelelőségi magatartásának megértését korlátozta az emberi viselkedés belső motivációjára való figyelem hiánya. Fontos következményekkel jár ez azoknak a munkaszervezeteknek, vezetőknek, információbiztonsági vezetőknek is, amelyek aggódnak az emberi funkciók kezeléséért a biztonsági műveleteik során: nagyobb hangsúlyt kell fektetni a belső motiváción alapuló megközelítésekre, mint a szankcióalapú megközelítésekre annak érdekében, hogy növeljük annak valószínűségét, hogy a munkavállalók megfelelnek az információbiztonsági szabályzatoknak. Ezen kívül azonban nem csak kizárólag a közigazgatásról, vagy az általános nemzeti kibertudatosságról van szó. Hanem további, legalább két szempontot is figyelembe kell venni, az állami információs szolgáltatásokba vetett bizalom és az e-kereskedelembe vetett bizalom is

sérülhet, ha az információbiztonsági alacsony tudásszint (mint kockázatot), kihasználhatják egyéni, vagy szervezett kiberbűnözők.

A nemzeti fejlesztés, és annak első lépése a mérés mellett szól, hogy speciális, nagymintás, geolokációs, egyéb változók is vizsgálhatóvá válnának, tehát nem zárható ki annak lehetősége, hogy egyes potenciálisan fontos változók hatásai lényegi plusz információval szolgálnának az oktatási stratégia fejlesztésében. Az eredmények erőteljesebbek lehetnek, ha kontrol alá lenne vonható más potenciálisan fontos változók, például a munkakör pozíciója, a munkakör egyéb jellemzői, és szakmai tagság, összességében minden lehetséges, kvantifikálható tényező, amely így már természetesen nem csak az adott munkaszervezetre és munkavállalókra, hanem geolókáció, szolgáltatási profil, stb. tényezőket is képes vizsgálni.

Mivel disszertációmban már volt szó szerepkörökről, így most a jobb érthetőség kedvéért itt példákon keresztül is bemutatom. A szerepkör alapú oktatás, oktatási csatornák fontossága bemutatásra került már. A szerepkör alapú oktatóknak két fontos alátámasztása van, mivel az oktatásokat, a szükséges lépéseket a kockázatok felmérése, kockázatarányosan kell megtenni, így eltérő szerepekben (munkakörökben) eltérő kockázatok lehetnek. Másrészről, eltérő munkakörök és szerepek eltérő munkafolyamatokat és tudást feltételeznek, így más - más, de legalábbis részlegesen más kockázatokra reagáló, azt megfelelően kezelni tudó, gyakorlatban alkalmazható tudásra van szükség, - túl az általános ismereteken - az egyes szerepkörökben.

Munkaszervezetenként eltérő szerepkörök lehetnek, erre csak a kockázatok (munkafolyamatok) felmérése során lehet pontos választ adni. Azonabn bizonyos szerepkörök tipizálhatóak, például megfigyeléseim alapján, ezeket egyes esetekben érdekelt felek (stakeholder) kifejezéssel is illethetjük:

- felsővezetés, menedzsment, pénzügyi, biztonsági, kiemelt vezető
    - tipikus kockázat CEO fraud, a felsővezetés (vagy bármely vezető) megszemélyesítése, nevében elkövetett visszaélés, utasítás adás
- középvezetők, csoportvezetők
    - akik képviselik a szervezeti normákat és saját példájukkal elől járnak, (bármi is az)
- pénzügyi tranzakciókban résztvevők
    - jóváhagyók, utalást feladók, belső partnerek,
- informatikai rendszerekhez kiemelt hozzáféréssel rendelkezők köre,
    - ide tartoznak a biztonsági rendszerek üzemeltetői, informatikusok, rendszergazdák, fejlesztők, bizonyos esetekben a beszállítók partnerek, (supply chain attack is elképzelhető)
- fizikai biztonságért felelős személyek
    - portás, biztonsági őr, beléptető rendszer üzemeltető,
- egyedi szerepkörök
    - kutatók, véleményvezérek,

- bennfentes típus
    - auditorok, ügyfelek, állandó vagy ideiglenes alkalmazottak, lízingelt vagy bérelt munkaerő, volt alkalmazottak és szállítók, külsős karbantartók, szakértő,
    -
- egyéb jogviszonyban foglalkoztatott munkavállalók, (ideiglenes, kölcsönzött, időszakos)
- egyéb számítógépes, információs rendszerekkel közvetlenül nem dolgozók köre,
- jogi szakterület,
- egyéb, az adott ágazatban vagy munkaszervezetben azonosítható, jelentős kockázattal azonosított szerepkör, munkakör

A szakirodalom alapján ezek egy részét stakeholderként azonosítottak, terjedelmi okokból az általam fentiekben ismertetett felosztást külön nem indoklom, ill. további példákat nem sorolok rá, egyrészt mert axiomaként kezelhető, másrészről az adott munkaszervezetben azonosított kockázatok alapján szükséges meghatározni, tehát ez csak mintaként szolgál.

A fentieken kívül természetesen egyéb tipizálható szerepkörök, vagy nem tipizálható egyedi jogkörök is lehetnek akár egyes közigazgatási szervezetekben, vagy más munkaszervezeteknél, vagy IT rendszerekben, akár azon kívül. Mindenesetre a fenti szerepkör felosztási modell alkalmas lehet arra, hogy akár az információbiztonsági szabályzat szerepkör alapú kivonatait ennek megfelelően készítse el az információbiztonsági szakterület.

Napjainkban nemzeti és munkaszervezeti szinten is, de általában véve a szervezetek számára a legfontosabb kérdés, az információbiztonsági szempontból az alkalmazottak szabálykövetési hajlandósága, vagy ha nem teljesítik az információbiztonság eljárásait. A dolgozatban ennek okairól már részletesen volt szó. Azaz visszavezethető

- csoportnyomásra
- időprésre, munkafolyamattal való ütközésre,
- szándékos károkozásra vagy nem szándékos hibára,
- tudás vagy információ hiányra,
- a tudás alkalmazhatóságának, azaz gyakorlati alkalmazásbeli tudáshiányra,
- apátia, hanyagság,
- egyéb, további

okokra.

Bagchi (2003) 2003-ban még arról írt, hogy a szervezetek általában évente legalább egy biztonsági incidenst tapasztalnak az információbiztonsági irányelvek megsértése miatt. Minden bizonnyal ez a szám azóta csak növekedett, egyrészt a növekvő kiberincidensek száma miatt, másrészről az eddig belügyként kezelhető incidensek egy (a személyes vagy különleges adatokat érintő) része jelentésköteles lett.

Becslések szerint az összes információbiztonsági szabálysértés több mint felét közvetetten vagy közvetlenül az okozza, hogy a munkavállalók nem tartják be az információbiztonsági eljárásokat

J. Stanton et al. (2005). Saját megfigyeléseim összevágnak a nemzetközi szakirodalommal, jelentős számú biztonsági incidenssel küzd meg egy átlagos szervezetben az információbiztonsági vezető.

Vance et al. (2012) szerint a szokáselmélet azt sugallja, hogy sok cselekvés tudatos cselekvési döntés nélkül következik be, és azért hajtódik végre, mert az egyének hozzászoktak ezek végrehajtásához; a gyakran ismétlődő magatartást inkább a szituációs jelek irányítják, mint a tudatos döntéshozatal. Megoldásként az vetik fel, hogy az új viselkedési minta megindításához (először) tudatos döntés szükséges, és az új viselkedés fokozatosan automatikus lesz. Tehát úgy vélem, hogy az információbiztonsági szabályzatnak való megfelelés szokásos viselkedése negatívan befolyásolhatja. Ugyanakkor ez az elmélet visszamutat arra, hogy a szokásnak fontos szerepe van az alkalmazottak információbiztonsági szabályzatnak való megfelelés összefüggésében. Így a szokásnak jelentős hatása van arra, hogy az alkalmazottak úgy érzik-e, hogy veszélyeztetettek, ha nem tartják be az információbiztonsági biztonsági szabályzatot; jelentős hatással volt a fenyegetés észlelt súlyosságára is, ha úgy vélték, hogy az IS biztonsági politikáinak betartása elősegítheti a biztonság megsértésének minimalizálását (reagálási hatékonyság), és ha képesnek érzik magukat az IS biztonsági eljárásainak betartására (önhatékonyság). Továbbá, ha egy személy úgy érzi, hogy az IS biztonsági eljárásai kellemetlenségeket okoznak (válaszköltségek), vagy ha úgy találja, hogy az ilyen eljárásoknak való megfelelés időt ad a „normális” munkafeladatok (jutalmak) elvégzésére, akkor az illető továbbra is fenntartja a hitét. Másodszor, a fenyegetés súlyossága pozitív hatással volt az alkalmazottak azon szándékára, hogy megfeleljenek az IS biztonsági politikájának… Nagyon fontos megállapításnak tartom, hogy az adott személynek fontos, hogy képesnek kell, hogy érezze magát a szabály betartására, az adott szabály követésre, vagy az adott eszköz használatára.
A szakirodalom alapján és véleményem szerint is fontos segíteni az alkalmazottakat a szabályzat megértésében, hogy a be nem tartás súlyos információbiztonsági problémákat okozhat szervezetük számára. A szervezeteknek információbiztonsági szemináriumokat vagy tréningeket kell szervezniük, ahol az alkalmazottak tájékoztatást kapnak a lehetséges információbiztonsági fenyegetésekről, valamint azok súlyosságáról és sebességéről. Olyan tipizálható jegyeket is meg kell ismertetni velük, amelyek alapján képesek az eszkalálódó problémát idejében felismerni és jelenteni. Tehát az, hogy ha egy tipizálható incidensre, hogyan reagál a munkavállaló, azon mérhető és egyébként tesztelhető is az információbiztonsági szabályalkalmazás (tudatosság) szintje.

Som (2014) a kritikus sikertényező közé sorolja a biztonsági tanács megalakítását és a szervezeti kultúrát, A vezetőség támogatásának fenntartása, megfelelő biztonsági tanácsi képviselet, valamint a végfelhasználói tudatosságot többek között. Vance et al. (2012).
Ezenkívül az információbiztonsági képviselőinek és általában a vezetőkenk terjeszteniük kell ezt az üzenetet beosztottaik között. A gyakorlatban is meg kell változtatniuk szervezeti kultúrájukat és munkakörnyezetüket, hogy ösztönözzék az információbiztonsági szabályzat betartását és azt inkább szükségszerűségnek, mint akadálynak érezzék, amely akadályozza az alkalmazottak munkáját. Nyilvánvaló, hogy az információbiztonsági gyakorlatok és eljárások nem lehetnek nehézkesek, mivel ez csak azt az érzetet kelti, hogy az információbiztonsági gyakorlatok betartása túl sok időt vesz igénybe. Ez az érzet negatívan befolyásolja az információbiztonsági szabálykövetési hajlandóságot.
Fontos annak biztosítása is, hogy az információbiztonsági szabályzat és gyakorlatok relevánsnak és könnyen használhatónak tartsák és azok is legyenek, amelyekre később az információbiztonsági szabályzat időbeli felülvizsgálata során még részletezek.

Safa et al. (2018) figyelmét is felkeltette ezen terület, tudományos irodalma már létezik, a bennfentes fenyegetéseknek. A bennfentes fenyegetések feltárásakor két különösen fontos szempont a motiváció és a lehetőség. Két alapvető elmélet jelenik meg a szakirodalomban a benfentes fenyegetésekkel kapcsolatosan, amelyek ezekre a jelenségekre vonatkoznak. A Social Bond Theory (SBT), magyar információbiztonsági szakirodaloma ennek sincs még, talán Társadalmi Kötelék Elmélet –nek nevezhető, amely felhasználható a rossz magatartás iránti motiváció gyengítéséhez. Ezen kívül a Situational Crime Prevention Theory Helyzetfüggő , vagy Szituációs Bűnmegelőzési Elmélet (SCPT) , amely alkalmas lehet arra, hogy felhasználható a helytelen viselkedés lehetőségeinek, döntéseinek csökkentésére. Beebe ls Rao (2005)

Safa et al. (2018) kutatása megállapítja, hogy a társadalmi kötelékténye zők, például a szervezeti politikák, szabályzatok és eljárások iránti elkötelezettség, az információbiztonsági tevékenységekben való részvétel és a személyes normák is jelentősen elősegítik a helytelen viselkedéssel szembeni negatív hozzáállás elfogadását.
A bennfentes fenyegetések veszélyeztetik az információk titkosságát, integritását és elérhetőségét. Padayachee (2012) A kritikus információk törlése, sokszorosítása, kiszűrése és jogosulatlan kinyerése példák az információ biztonsági fenyegetéseire ezen a területen, és ezeknek a gyökereknek a gyökerei az apátia, megvesztegetés, korrupció, kémkedés, sikkasztás, zsarolás, tudatlanság és szabotázs Turkanovi et al. (2013) szerint. Elismert tény, hogy a motiváció és a

lehetőség egyaránt döntő szerepet játszik az információbiztonsági szabályok és előírások megsértésében Padayachee (2012) szerint.
Az információbiztonsági bennfentes fenyegetések területe a szervezetekben elsősorban az alkalmazottak attitűdjeire, szándékaira és viselkedésére összpontosít. A bűncselekmények kényelmessége és az ahhoz való mozgás kényelme, azaz a lehetőség és a körülmények, kockázatok előnyök érzékelése fontos szerepet játszik az alkalmazottak bűnözői viselkedésének etiológiájában Padayachee K. (2013) szerint.

Safa et al. (2018) bennfentes fenyegetések enyhítésére vonatkozó modellre két fontos megközelítésen alapszik: a bűncselekmények elkövetésének lehetőségének csökkentésére és az alkalmazottak motiválttá tételére a nem megfelelő viselkedés elkerülésére. Meglátásom szerint ez jól összefoglalja azokat a lehetséges információbiztonsági feladatokat amit az információbiztonsági terület meg tud tenni a bennfentes fenyegetések kockázatának csökkentés érdekében. Som (2014) úgy fogalmaz, hogy a hatékony program kidolgozáshoz számtalan tényezőt érdemes figyelembe venni, ahhoz, hogy a program valóban jól működjön az adott szervezetben. Tehát bár a kockázat felméréshez és értékeléshez Som (2014) közread egy mintát, de felhívja a figyelmet annak szervezetre szabási fontosságára.
A bennfentes fenyegetéseket, csak a szükséges mélységben vizsgálva még meg kívánom említeni, hogy Safa et al. eredményei azt iis feltárták, hogy a szervezet információbiztonsági szabályzata iránti elkötelezettség ($\beta = 0{,}742$, $p = 0{,}004$), részvétel az információbiztonsági tevékenységekben ($\beta = 0{,}689$, $p = 0{,}016$) és a személyes normák ($\beta = 0{,}516$, $p = .014$) jelentős hatással vannak a helytelen viselkedéssel kapcsolatos negatív hozzáállásra, azonban a munkaszervezethez való kötődés nem befolyásolja jelentősen az attitűdöt. Továbbá azt is megállapíttotta, hogy a helytelen viselkedéssel szembeni negatív hozzáállás ($\beta = 0{,}718$, $p = 0{,}001$) jelentősen csökkenti a helytelen viselkedési szándékot, a visszaélési szándék csökkenése ($\beta = 0{,}698$, $p = 0{,}001$) viszont jelentősen csökkenti a bennfentes fenyegetéseket.

A fentebb megfogalmazott két módszerhez kapcsolódóan, a bennfentes fenyegetések csökkentésére megoldás lehet, a titkosítást, az automatikus adatmegsemmisítő mechanizmusokat és az események folytonosságának kezelését szintén hatékony megközelítésként kínálják, amelyek csökkentik az elérhető előnyöket. Li et al. (2010) szerint különösen igaz az akkor, ha az elkövetők lopott adatok értékesítését tervezik Li et al. (2010). Tehát nem elég a megfelelő szabályzatok és technikai kontrollok alkalmazása, de ezek kommunikációs és transzparenciája is szükséges, legalább annyira hatékony visszatartó erő lehet meglátásom szerint. Li et al. (2010)

ennek alapján feltételezi, hogy a jutalom csökkentése visszatartja a munkavállalókat a szervezetekben elkövetett helytelen magatartástól. Az információbiztonsági helytelen magatartással járó elérhető nyereségek csökkentése befolyásolja az alkalmazottak hozzáállását az alkalmazottak szándékának csökkentéséhez az információbiztonsági helytelen viselkedés iránt. Meg kell jegyezni, hogy a hanyagságból, nem értelmezhető mennyiségű nyereségből elkövetett eseményekre ez nem biztos, hogy alkalmazható.

Véleményem és kutatási eredményeimre hivatkozással, valamint a szakirodalom Safa et al. (2018) is alátámasztja, miszerint az információbiztonsági programokban való részvétel csökkenti a bennfentes fenyegetéseket, ahol a munkatársak részvétele az információbiztonsági tevékenységekben különböző formákban történhet, például: információbiztonsági ismeretek megosztása, információbiztonsági együttműködés és információbiztonsági tapasztalatok. Safaa et al. (2018) Fontos kiemelnem, hogy ilyen programoknak tekinthető véleményem szerint a disszertációmban említett formális képzési formák mellett az informális eszmecsere (pletykát) vagy bármilyen olyan informális impulzust amelyet egymás között osztanak meg a munkavállalók, vagy központilag történik a megosztása.

16. SZÁMÚ MELLÉKLET, A STRESSZ HATÁSA AZ INFORMÁCIÓBIZTONSÁGRA

A korábban említetteken kívül a munkavállalóknak, mint az információs rendszereket (biztonságosan) üzemeltetni szándékozó személyeknek különféle helyzeteket szükséges kezelniük, amelyekben a szervezet információbiztonsági célkitűzései akadályozhatják a dolgozók azon célkitűzéseit, hogy a feladataikat hatékonyan tudják elvégezni, ami további stresszt okozhat bennük és negatívan befolyásolhatja a biztonsági előírások betartását. A kérdés időbeli síkon és változások tekintetében vizsgálva pedig a munkavállalóknak meg kell küzdeni az információs technológia folyamatos változásai által okozott kihívásokkal Inho Hwang (2018). Ebben az alfejezetben azt mutatom be, hogy egyes szerepkörökben, milyen lehetséges stressz típusok merülhetnek fel, amelyek befolyásolhatják az információbiztonsági szabályalkalmazási képességet.

A szerepstressz alatt a munkahelyen érzékelt körülmények vagy események eredményeként felmerülő személyes diszfunkció tudatosságát vagy érzetét, valamint az ilyen kényelmetlen, nemkívánatos vagy fenyegető munkahelyi körülményekből adódó pszichológiai és élettani reakciókat értjük Jamal (1990) valamint Parker, és DeCotiis (1983) A szerepstressz két fő oka a szerepkonfliktus (role conflict) és a szerep kétértelműsége (role ambiguity). A szerepkonfliktus a szerepkövetelmények összeegyeztethetetlenségének észlelése Galluch, Grover, & Thatcher (2015), és akkor fordul elő, amikor egy alkalmazottat túl nagy mennyiségű feladat elvégzésére kéri a szervezet Tarafdar et al. (2007). A szerep kétértelműsége a szerep teljesítmény következményeinek kiszámíthatatlansága és a szerep elvégzéséhez szükséges információk hiánya Ayyagari, Grover, & Purvis (2011); Behrman & Perreault (1984). Példaként elegendő a közigazgatásban előforduló gyakorlatra gondolni, amikor meglévő munkavállaló, meglévő feladatai mellé plusz feladatként kapja meg az Információbiztonsági felelős pozíciót; esetleg képzettség hiányát vagy más nehezítő körülményeket nem említve. Vagy ha az informatikai üzemeltetői funkció mellé egy személyhez kerül az információbiztonsági szerepkör. További példaként meg kívánom említeni számos Magyarországi szervezetnél tapasztaltak alapján, hogy az új belépő munkavállalók oktatása, mind informatikai, mind információbiztonsági területen nem vagy csak részlegesen valósul meg, vagy az oktatás valamilyen hiányt szenved. Ez az oktatás vagy nevezhetjük transzparens támogatásnak az egyes szervezetekben a későbbiekben nem áll rendelkezésre. Így a munkavállaló belépéskor nem kapja meg a megfelelő kulturális lenyomatot, egyoldalú (csak a közvetlen kollégái által közvetített) csoportnyomást kap; Nem utolsó sorban kérdéseivel, támogatási igényével nem tud hova fordulni, így stressz alakulhat ki.

Az információbiztonság technológiai környezete befolyásolhatja a szerepkonfliktus és a szerep kétértelműségét, annak mértékét azon munkavállalók körében, akiknek meg kell felelniük a szervezet biztonsági követelményeinek, valamint saját munkakövetelményeiknek is. A legtöbb munkavállaló számára a munkahelyi céljainak elérése az elsődleges prioritás, ugyanakkor az információbiztonsági irányelvek betartása nem feltétlenül szerepel saját listájuk élén. Disszertációban bemutatásra kerülő eredmények is alátámasztják ezt, hogy az információbiztonsági szabályzat nem ismert kellő mértékben a munkavállalók körében, az információbiztonsági szabályzatnak szerepkör alapú kivonatai csekély mértékben állnak rendelkezésre.

A szervezetek tehát megkövetelik az alkalmazottaktól az információbiztonságnak való megfelelést, amely esetleg nem kompatibilis az alkalmazottak munkafolyamataival. Például egy olyan feladat elérése érdekében, ami egy külső partnerrel időben megkötött megállapodással kapcsolatos és amely fontos dokumentumok cseréjét igényli, a biztonsági előírások összetett technológiai eljárásokat írhatnak elő amelyek befejezése akár napokba is telhet. Ebben az esetben a munkavállaló nagymértékű konfliktust élhet meg a saját munkájából adódó cél, valamint a biztonsági követelmények által elvárt cél között. Hu et al. (2011) szerint is Ha a biztonsági megfelelés célja és iránya rosszul illeszkedik a szervezet egyéni céljaihoz, és a biztonsági követelmények hajlamosak további munkaterheket róni az emberekre, akkor szerepkonfliktusok merülhetnek fel a szervezet biztonsági követelményei és az alkalmazottak munkakövetelményei között.

Ezenkívül, amikor egy szervezet biztonsági követelménye az információbiztonsági technológia fejlesztéséből kifolyólag megváltozik, általában információhiányt és zavart okoz az alkalmazottak számára, ami a szerepkör félreérthetőségéhez (role ambiguity) vezet. Például, ha egy szervezet azt akarja, hogy alkalmazottai a PC-ről a mobil eszközökre váltsanak a munka elvégzéséhez, az információbiztonsági technológiai követelményt módosítják, hogy megfeleljen egy ilyen változáshoz. A munkavállalók egy ilyen esetben nem biztos, hogy tisztában vannak az új technológiával, az információbiztonsági követelményekkel vagy azokkal a forrásokkal, ahonnan segítséget kaphatnak a változással kapcsolatban, (IKT technológiai, folyamatokat érintő és információbiztonsági tekintetben is értve) vagy azokkal a forrásokkal, ahonnan tájékozódhatnak a szabályzatokról, változásokról, számukra érthető módon. Ez pedig a stressz forrása lehet. Vakola, M., & Nikolaou, I. (2005) megállapítja, hogy az ilyen stressz negatívan hat a szervezeti

elköteleződésre. Így egy információbiztonsági oktatáshoz szükséges lehet a meglévő és a szükséges informatikai kompetenciák felmérése és kialakítása. (Bujdosó, 2014)

Meg kell említeni még a téma kapcsán D'Arcy et al. (2014) nevét, mivel tanulmánya azon kevés tanulmány egyike volt, amely bevezette a technostress fogalmát az információbiztonsági irodalomba. A biztonsággal kapcsolatos stressz (Security Related Stress, SRS) név felhasználásával rámutattak a technostress fontosságára, és bemutatták az SRS és az információbiztonsági szabályzat megsértési szándékának kapcsolatát. A szakirodalmi áttekintés és megfigyeléseim alapján a tapasztalatok azt mutatják, hogy a technostress létrehozók növelik a munkahelyi szerep stresszt, Ayyagari, R., Grover, V., & Purvis, R. (2011) és ez alól az információbiztonsági technológiával kapcsolatos körülmények sem kivételek. Az információbiztonsági technológia bonyolultabbá és speciálisabbá válásával az alkalmazottak, akiknek az információbiztonsági technológiákkal kapcsolatos követelményekkel kell foglalkozniuk munkafolyamataik különböző szakaszaiban, várhatóan megnövekedett szerepkonfliktust és szerep bizonytalanságot (role ambiguity) élhetnek meg.

Gyakorló információbiztonsági szakemberként pedig alátámasztottnak találtam azokat a szakirodalmi példákat, amelyek azt igazolják, hogy stressz faktor a szabályzatok naprakész ismeretének és alkalmazásának elvárása, így például, de nem kizárólag, hogy gyakran a szabályzatok elolvasására nincs idő, megértése a szakszavak miatt nehézkes, vagy mert teljesen eltérő szakterületeken dolgozó, eltérő előképzettségű embereknek nem szerepkörre szabottan készülnek ezen leírások, terjedelmük terjengős, s mindezeket olyan mélységben kellene megérteni, hogy saját szakterületükre azt alkalmazni is tudják. Ugyanakkor ezen igényeknek való megfelelés a gyakorlatban jellemzően nem érvényesül, szerepkör alapú kivonatko alacsony száma miatt, illetve Elham Rostami (2019) megállapítja, hogy a szabályzatalkotás folyamatába nem megfelelő mértékben vonják be az egyes szerepkörökben dolgozó, de általában véve a munkavállalókat. E miatt a szabályzatokban foglaltak nem tükrözik a felhasználói megértést támogató információkat, azok alkalmazása így kevésbé lehetséges.
Fel kell tennünk a kérdés, hogy mit jelent a szabályzatokban foglaltak alkalmazása. Voltaképpen belátható, hogy a szabályzat aktuális verziójának megtalálása, elolvasása, annak megértése és olyan mértékű elsajátítása, hogy saját folyamataiban és szakterületén alkalmazni tudja a munkavállaló. Lássuk be hogy nem tud esetleg döntést hozni, tehát annak felismerése, hogy támogatásra van szüksége. Így egy szakmai támogatást nyújtásra van szükség, amely gyakran

technikai ismeretek nélküli, „csak” kijelölt, egyszemélyi információbiztonsági vezetői pozícióban valósul meg.
A technikai ismeretek hiányát azért szükséges kihangsúlyozni, Stanton et al. (2004) sőt pontosítani, hogy az aktuálisan adott szervezetben alkalmazott technikai megoldások és ebben a környezetben létrehozható kompenzációs kontrollokról van szó, mivel az lehet válasz a feltett kérdésre. Így példát mutattam arra, hogy nem csak felhasználói, de minden egyes szerepkörre általánosíthatóak a fentiekben megfogalmazott stressz típusok és kritériumok.

Az eddigieket összegezve megfogalmazható, hogy az információbiztonsági technológia és az ebből adódó szerep-stressz okozta stresszhatások negatív hatással lehetnek az információbiztonsági megfelelésre vonatkozóan, mivel ronthatja a munkavállalók elkötelezettségét szervezeti célok iránt. A szervezeti elkötelezettség alatt azt értjük, hogy a munkavállalók milyen mértékben hajlandóak hinni és azonosulni a szervezettel, annak célkitűzéseivel Meyer, J. et al. (2002) szerint. A magasabb szintű szervezeti elkötelezettséggel rendelkező alkalmazottak hajlamosak integrálni magukat a szervezet céljaival (Stanton et al, 2004). A szakirodalom azt mutatja, hogy a biztonsággal kapcsolatos technológia növekvő nyomása és a megnövekedett szerep-stressz komoly források lehetnek a szervezeti elkötelezettség aláásására, ez pedig elvonja az alkalmazottakat azon szervezeti céloktól amelyek azt elősegítenék, az információbiztonsági előírások betartását. Példaként (Inho Hwang, 2018) is azt állítja, hogy a szervezeti elkötelezettség közvetítőként történő felhasználásával az alkalmazottak információbiztonságnak való megfelelése nem csupán egyéni döntés kérdése a munkavállalók saját erkölcsi normáinak megfelelően, vagy az előnyök és hátrányok személyes elemzése; inkább egy olyan döntés, amely magában foglalja a szervezettel fennálló kapcsolataikat, azaz azt, hogy azonosuljanak-e a szervezettel, és annak információbiztonsági céljaival.

A szervezeteknek tehát fontolóra kell venniük az információbiztonsági technológiák alkalmazóinak technostressz és szerep stressz kezelését, mint egy fontos stratégiát az információbiztonság javítására és a szervezeten belüli szereplők által előidézett biztonsági szabálysértések és események csökkentésére. Ennek első állomása ezen indikátor mérése, kiértékelése lehet. Amelyből egy lehetséges második lépés lehet, az információbiztonsági technológiák alkalmazóinak megfelelő és célzott támogatása.

Más tanulmányok olyan munkavállalói vélekedéseket tárták fel a biztonsági követelményekről, amely szerint azok nehezen érthetőek és összeegyeztethetetlenek az alapvető munkaköri feladatokkal.

Ugyanakkor a legmodernebb, általam is képviselt megközelítés szerint a szerepkör alapú kivonatok, a széles spektrumú, de fókuszált támogatás, érthető és figyelemfelkeltő, (megragadó) kommunikáció kérdésfeltevésre sarkalhat az ellenállás helyett. Kiegészítve a könnyű kérdésfeltevési, visszajelzési, támogatáskérési lehetőséggel. Ennek következménye lehet az összeegyeztethetőség keresése a biztonsági követelményeknek a munkaköri feladatokkal. Az egyes követelményekhez (lehetőség szerint) olyan plusz addicionális információ csatolása, amely a személyes kapcsolódást (bevonódást) segíti elő, azaz így akár magánéletben használhatóságát is akár. Az információbiztonsági szabályzat közzététele és kétirányú kommunikációs csatorna, azaz támogatás biztosítása a megértéshez, betartáshoz. Valamint ezen csatornán, csatornákon keresztül kapott visszajelzések, észrevételek jó indikátorok lehetnek.

Az SRS következményeit illetően számos szerző megállapításai azt sugallják, hogy az ISP megfelelése csökken, ha a biztonsági követelményeket a munka akadályának (stresszes állapotnak) érzékelik az alkalmazottak az általuk erre felhasznált idő és erőfeszítés miatt.

A frusztráció érzése arra is ösztönözheti az alkalmazottakat, hogy lazábban álljanak hozzá a belső normáik elvárásaihoz, amelyek amúgy tiltanák az információbiztonsági szabályzat megsértését, ezáltal megkönnyítve ennek a viselkedésnek a racionalizálását. Ezt a álláspontot támasztja alá M.H. Bazerman, A.E. Tenbrunsel (2011) kutatása, amely a munkavállalói frusztrációt a munkahelyi etikátlan magatartás iránti fokozott toleranciához (gyakorlathoz) tudta kapcsolni .

17. SZÁMÚ MELLÉKLET, FELHASZNÁLÓI TUDATOSSÁG ÉRETTSÉGI MODELLJE

A Felhasználói Tudatosság Érettségi Modelljét (User Awareness Maturity Model - UAMM) Steve Kruse és Bill Pankey mutatták be. Ők az informatikai rendszerek felhasználóit, azaz a felhasználókat sorolták be tudatosság szempontjából és ahogy már megszokhattuk egy ötfokozatú skálán: Tarján (2018) így foglalja össze ezt az 5 pontot:

1. Fokozat: „a szerencsés tudatlan” (blissfully unaware)

· Ez a személy nem ismeri fel, illetve nem tekinti valósnak az információbiztonsági fenyegetéseket, ezért ezek figyelembevétele nélkül használja a különféle eszközöket és erőforrásokat.

· Az ezen a szinten lévők vélekedése szerint az információbiztonság nem az egyéni felhasználó viselkedésének függvénye, hanem az IT rendszerekhez kapcsolódó konfigurációs kérdés.

2. Fokozat: „a tudatosan inkompetens” (consciously incompetent)

· Az a személy, aki akár a termelékenység rovására is tartózkodik a túl kockázatosnak vélt cselekvéstől.

3. Fokozat: „a megfelelőségre törekvő” (compliant)

· Számára világosak azok a kockázatok, amiket a szervezeti szabályozás rögzít.

· A szabályzat előírásait követi minden olyan esetben, amelyre van szabályzati protokoll.

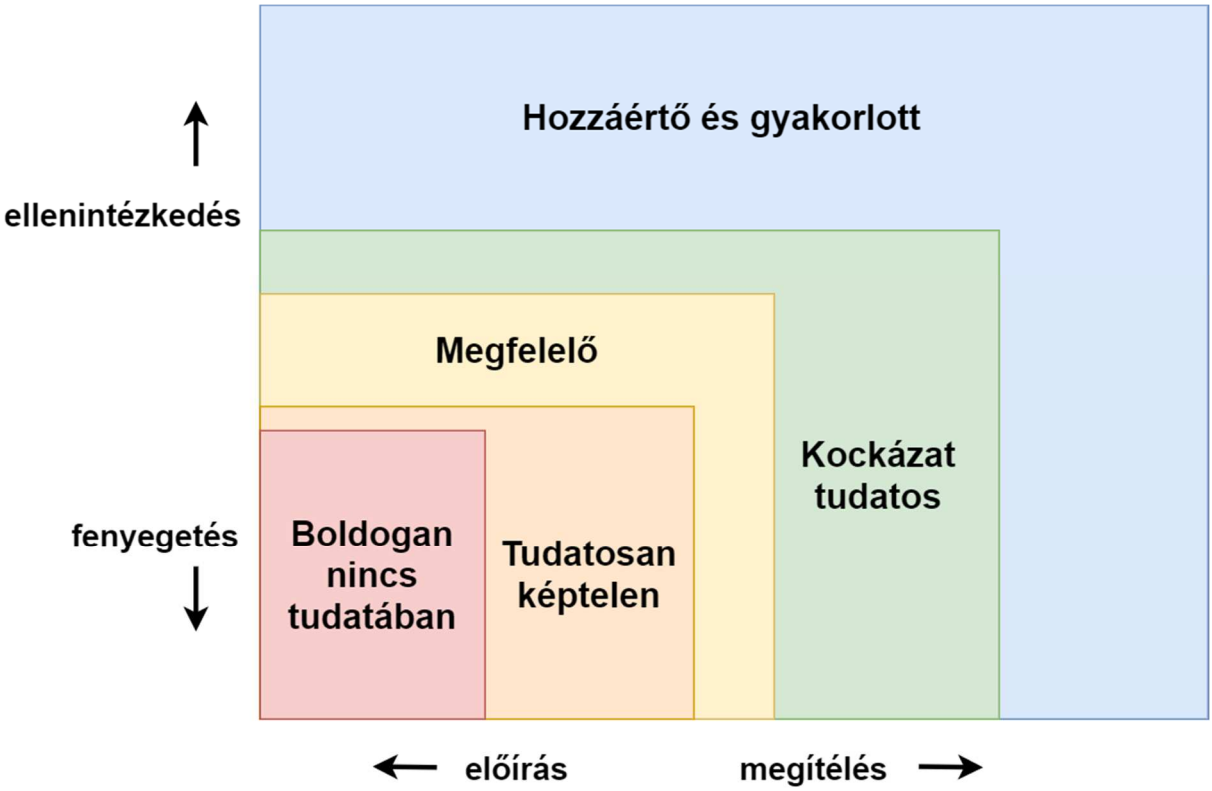
4. Fokozat: „a kockázat tudatos” (risk aware)

· Tekintettel van azokra az információbiztonsági kockázatokra, melyek a szervezet működését veszélyeztetik, ám olykor bizonytalanul jár el, ritkán tesz jelentést.

5. Szint: „a kompetens és gyakorlott” (competent & practiced)

· Észleli és mérsékeli az információbiztonsági kockázatokat úgy, hogy mindeközben munkaköri kötelezettségeinek is eleget tesz.

Az UAMM két dimenzió mentén helyezi el az alkalmazottakat az adott érettségi szinteken.



83. ábra: , A Felhasználói Tudatosság Érettségi Modellje - UAMM (2018) p. 7

Az 83. számú ábráról leolvasható, hogy

· A vízszintes tengelyen a felhasználó viselkedését értékeljük az alapján, mennyire megfontolt. Érettségének növekedése révén nagyobb teret engedhetünk a felhasználónak.

· A függőleges tengely a kockázatmenedzselési felelősséget mutatja, amely egyenes arányban növekszik a felhasználó érettségi szintjével.

Habár UAMM egyes személyek érettségi szintjéről beszél, Kruse és Pankey megfogalmazásaiból azt a következtetést vonhatjuk le, hogy ők az embereket (stakeholder) mint informatikai rendszerek felhasználóit tekintik. Mi azonban, amikor a tudatosság kérdéskörét tárgyaljuk, nem csak informatikai eszközök, berendezések kezelőire koncentrálunk.

Ebből a megközelítésből disszertációmban nem korlátozom le és nem számszerűsítem a lehetséges szerepköröket. Hanem az adott munkaszervezetben, a kockázatfelmérés alapján és munkafolyamatok figyelembevételébel szükséges azokat meghatározni, szerepkör alapú tréninget tartani. Valamint ahogy kifejtem az információbiztonság a számítógépes hozzáféréssel formálisan nem rendelkező munkavállalókra és stakeholdrekre is ki kell, hogy terjedjen.

Lance Spitzer volt az, aki először mutatta be a SANS Institute Információbiztonsági Tudatossági Érettségi Modelljét (Security Awareness Maturity Model) egy blogbejegyzésben (2012. május

22.). A modellen idővel többször módosítottak, de eredetileg egy öt lépcsőből álló megközelítést tartalmazott, ezt írja le Spitzer.

Tarján (2020) Az információbiztonsági tudatosság érettségi szintjének mérési problémái gazdálkodó szervezetekben című tanulmányában szintén bemutatja a modellt, melynek felépítését röviden összefoglalom:

· 1. szint: Nincs információbiztonsági tudatosító program

Ha nincs program, nem kerül sor a szervezet tagjainak képzésére. Ebből az következik, hogy a szervezi tagoknak nincsen tudomása a szervezeti szabályokról, eljárásokról, így nem is értik azokat. Az ilyen szervezet ki van téve a támadásoknak, mivel a tagok nincsenek tudatában sérülékenységének.

· 2. szint: Megfelelőségre fókuszáló program

Ez egyfajta tudatosító program, amely nem a viselkedés megváltoztatását célozza, hanem a megfelelőséggel és a felülvizsgálati követelmények teljesítésével kapcsolatos. Jelenthet éves gyakoriságú vagy rendszertelenül szervezett tantermi előadásokat, máskor kimerül negyedévente érkező hírlevelek formájában. A program nem éri el azt a célt, hogy az alkalmazottak kellő biztonsággal értelmezzék a szervezeti szabályokat vagy saját felelősségüket a szervezeti információk megóvásában, és a biztonsági incidensek megelőzésével és kezelésével kapcsolatban is bizonytalanok.

· 3. szint: A tudatosítás és változás promóciója

Ez a szint már a viselkedés megváltoztatását célozza, így törekszik a szervezeti kockázatok csökkentésére. Mivel elérése az előző két szintnél lényegesen nehezebb, a szervezetek túlnyomó része nem jut el idáig. A program ezen a szinten olyan kérdéseket állít középpontba, amelyek leginkább meghatározóak a szervezeti célok megvalósulásánál, így túllép a különböző információs anyagok véletlenszerű terjesztésénél. Nem évenkénti előadásokra, hanem folyamatos megerősítésekre épül, hogy motiválja a viselkedés megváltozását mind a munkahelyi, mind az otthoni környezetben, mind egy-egy utazás alkalmával. A szervezet dolgozói minden szinten tisztában vannak annak szabályaival, belső folyamataival, így aktívak az incidensek megelőzésében és kezelésében.

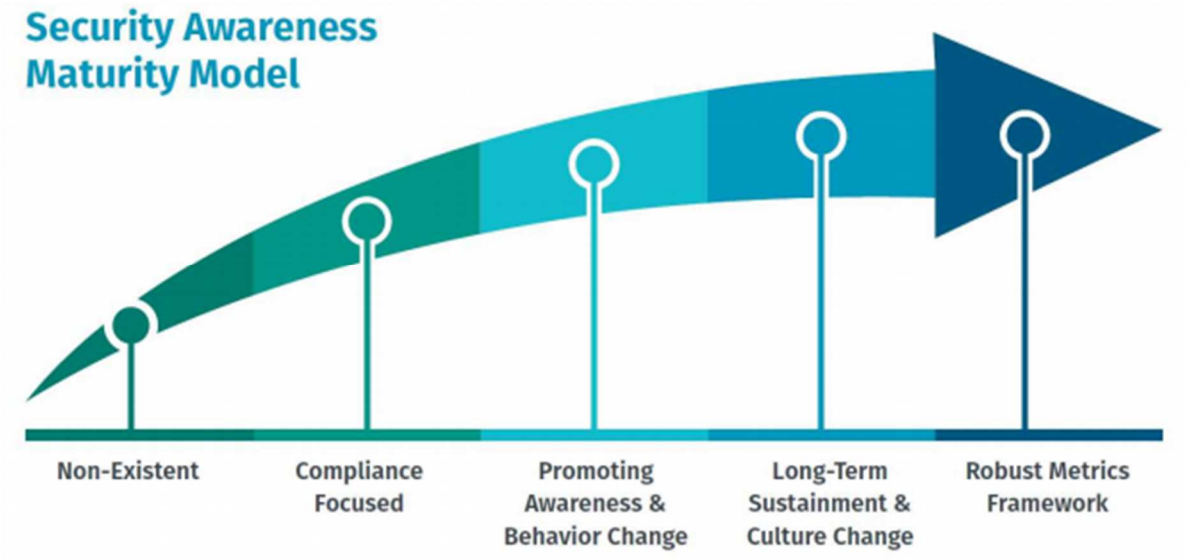
· 4. szint: A hosszútávú fenntarthatóság állapota

A program a tudatosság és a változás tartós fennállását célozza. Hosszútávú ciklusokat követ, melyek során a programot a fennálló folyamatokhoz és erőforrásokhoz igazítják. A kommunikációs módszerek és a kommunikált tartalmak hatékonyságát az éves felülvizsgálatok, szükség szerinti módosítások biztosítják. Ezáltal maradhat a program mindig aktuális és elfogadható – a szervezeti kultúrához igazodik, annak részét alkotja.

5. szint: Mérőszámok

A legfelsőbb szinten az előrehaladás, a biztonsági tudatosító program hatása már mérhetővé és követhetővé válik. Ez magában foglalja a program folyamatos fejlődését. A mérés lehetővé teszi a ráfordítás megtérülésének kimutatását is. Habár az alacsonyabb szinteken is lehetőség van mérések bevezetésére, de ezen a szinten a mérés már formalizált és programszerű. [7]

A leírtakhoz pár kisebb módosítással, ami a különböző szintek megnevezését érinti, kapcsolható a SANS Institute legutóbbi Információbiztonsági Tudatossági Jelentése (Security Awareness Report 2017) is.



84. ábra: az információbiztonsági tudatosság érettségi szintjei Forrás: Security Awareness Report 2017

Ezt a 84. számú ábrán látható modellt kezdetben abból a célból alkották, hogy értékelni tudják az információbiztonsági tudatosító programok érettségi szintjét.

Az ISO/IEC 27004:2016 „Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation" nemzetközi standardnak, szabványnak tekinthető dokumentum úgy fogalmaz, hogy célként határozza meg, hogy az információbiztonsági mérések útmutatásokat nyújt a szervezeteknek az információbiztonsági teljesítmény és az információbiztonsági irányítási rendszer hatékonyságának értékelésében, az ISO / IEC 27001: 2013, 9.1 követelményeinek teljesítése érdekében. A szabvány létrehozza:

a) az információbiztonsági teljesítmény figyelemmel kísérését és mérését;

b) az információbiztonsági irányítási rendszer (ISMS) hatékonyságának figyelemmel kísérése és mérése, ideértve annak folyamatait és ellenőrzéseit is;

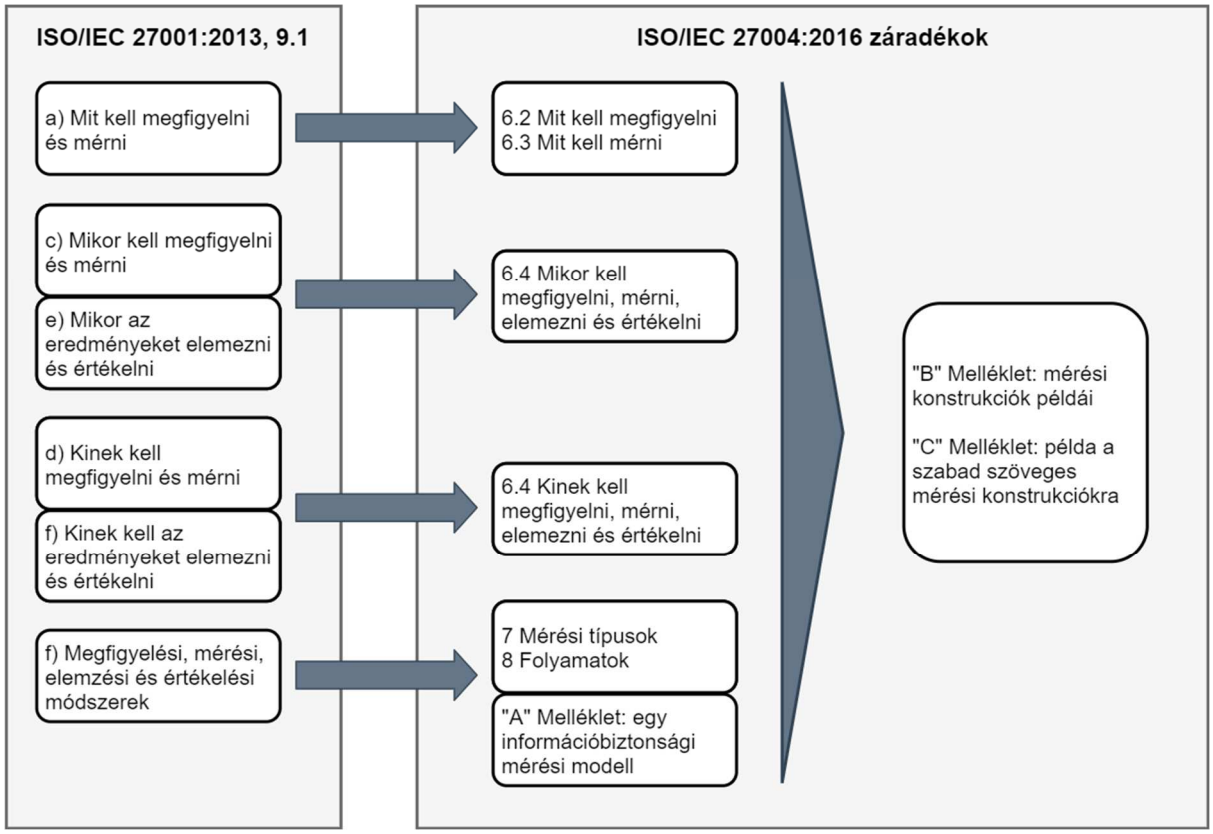
c) a monitoring és mérés eredményeinek elemzése és értékelését.

Valamint úgy fogalmaz, hogy a szabvány, a dokumentum minden típusú és méretű szervezetre alkalmazható.

Talán kevéssé szükséges indoklása a mérés szükségességének, azonban axiomatikus módon választ adva a kérdésre, az mondható, hogy az ISMS általános célja a hatálya alá tartozó információk bizalmasságának, integritásának és rendelkezésre állásának megőrzése. Vannak olyan ISMS tevékenységek, amelyek ennek megvalósításának tervezésével és e tervek végrehajtásával foglalkoznak. Ezek a tevékenységek önmagukban azonban nem garantálják, hogy e tervek megvalósítása megfeleljen az információbiztonsági céloknak. Ezért az ISO / IEC 27001 által meghatározott ISMS-ben több követelmény is fel van mérve, hogy a tervek és tevékenységek biztosítják-e az információbiztonsági célok teljesülését.

Felmerül a kérdés, hogyan biztosítja a szabvány az ISMS működését. Az ISO / IEC 27001: 2013, 9.1 előírja, hogy a szervezet értékelje az információbiztonsági teljesítményt és az ISMS hatékonyságát. Az ezen követelményeknek megfelelő intézkedéstípusok a 7. szakaszban találhatók.
Az ISO / IEC 27001: 2013, 9.1 előírja továbbá, hogy a szervezet határozza meg:
a) mit kell ellenőrizni és mérni, ideértve az információbiztonsági folyamatokat és ellenőrzéseket is;
b) adott esetben a nyomon követés, mérés, elemzés és értékelés módszerei az érvényes eredmények biztosítása érdekében;
c) mikor kell elvégezni az ellenőrzést és a mérést;
d) kik figyelik és mérik;
e) mikor kell elemezni és értékelni a monitoring és mérés eredményeit; és
f) ki elemzi és értékeli ezeket az eredményeket.
Ezen követelmények feltérképezését a 85. számú ábra tartalmazza.

Végül az ISO / IEC 27001: 2013, 9.1 előírja, hogy a szervezetnek meg kell őriznie a megfelelő dokumentált információkat a monitoring és mérési eredmények bizonyítékaként (lásd 8.9.).
Az ISO / IEC 27001: 2013, 9.1 azt is megjegyzi, hogy a kiválasztott módszereknek összehasonlítható és reprodukálható eredményeket kell hozniuk ahhoz, hogy érvényesnek lehessenek (lásd 6.4.).



85. ábra: Az ISO/IEC 27001:2013 9.1 pontjának követelményeivel összerendelése, Forrás: ISO/IEC 27004:2016 szabvány és 27001:2013 szabvány

Fontosnak tartom megemlíteni, hogy a szabvány 2013-as változatával számos dokumentációs kényszer kikerült, de az a kevés ami megmaradt, egyértelmű követelmény, hogy „dokumentált információt” tartson fenn a szervezet.
Meg kell említeni, hogy természetesen a gyűjtött információkat ki kell értékelni, értelmezni szükséges adott kontextusban, stb. számos teendő van amely lényegesen képes befolyásolni, hogy mennyire képes a szervezet hasznosítani a megszervezz, rendelkezésre álló információkat, méréseket.

Ami talán még hangsúlyosabb, hogy milyen előnyök származhatnak a mérésből, annak kiértékeléséből, megfelelő feldolgozásából.

Az információbiztonsági irányítási (ISMS) folyamatok és ellenőrzések teljesítése és az információbiztonsági teljesítmény biztosítása számos szervezeti és pénzügyi előnyt jelenthet. A fő előnyök a következők lehetnek (ISO/IEC 27004:2016 alapján):
a) Fokozott elszámoltathatóság: A megfigyelés, a mérés, az elemzés és az értékelés növelheti az információbiztonság elszámoltathatóságát azáltal, hogy elősegíti a helytelenül végrehajtott, nem végrehajtott vagy hatástalan konkrét információbiztonsági folyamatok vagy ellenőrzések azonosítását.
b) Javított információbiztonsági teljesítmény és ISMS folyamatok: A monitorozás, mérés, elemzés és értékelés lehetővé teheti a szervezetek számára, hogy számszerűsítsék az információbiztonság javulását az ISMS-ük körében, és számszerűsíthető előrelépést mutassanak a szervezet információbiztonsági céljainak megvalósításában.
c) Bizonyíték a követelmények teljesítéséről: A monitorozás, mérés, elemzés és értékelés dokumentált bizonyítékot nyújthat, amely segít bizonyítani az ISO / IEC 27001 (és más szabványok) követelményeinek, valamint az alkalmazandó törvényeknek, szabályoknak és előírásoknak való megfelelést.
d) A döntéshozatal támogatása: Az ellenőrzés, mérés, elemzés és értékelés támogathatja a kockázatalapú döntéshozatalt, számszerűsíthető információkkal hozzájárulva a kockázatkezelési folyamathoz. Lehetővé teheti a szervezetek számára, hogy mérjék a korábbi és a jelenlegi információbiztonsági beruházások sikereit és kudarcait, és számszerűsíthető adatokat kell szolgáltatniuk, amelyek támogathatják az erőforrások elosztását a jövőbeli beruházásokhoz.

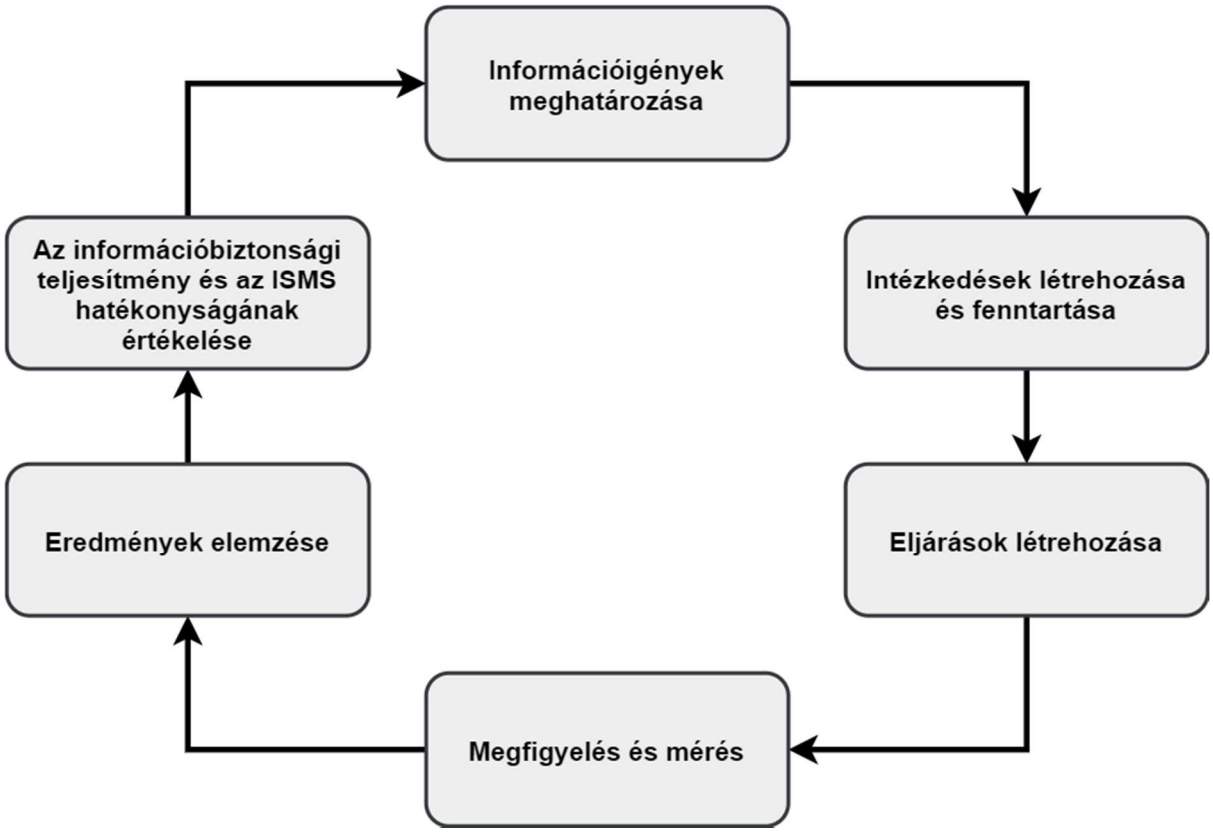
Mivel dolgozatomban nem kizárólag, sőt nem kifejezetten a mérés módszertanával foglalkozom, így csak röviden, de ismertetem azokat a kihagyhatatlan kérdéseket, mérföldköveket, amelyeket egy mérés – kiértékelés – döntés ciklus során meg kell tenni.

Bár a megfigyelés és a mérés az információbiztonsági teljesítmény és az ISMS hatékonyságának értékelésének első lépése nem az információbiztonsággal kapcsolatos entitások elsöprő sokféle mérhető attribútumával szemben nem teljesen nyilvánvaló, hogy melyiket kell mérni.
Ez azért fontos kérdés, mert kivitelezhetetlen, költséges és kontraproduktív a túl sok vagy a rossz tulajdonság mérése, vagy túl sok haszontalan információ feldolgozása. A számos tulajdonság mérésének, elemzésének és jelentésének nyilvánvaló költségeitől eltekintve egyértelműen fennáll annak a lehetősége, hogy a kulcsfontosságú kérdések elfedhetők nagy mennyiségű információ esetén, vagy egyáltalán kiértékelésük elmaradhat, ha nincsenek megfelelő intézkedések.

Annak meghatározása érdekében, hogy mit figyeljen és mérjen, a szervezetnek először meg kell fontolnia, hogy mit szeretne elérni az információbiztonsági teljesítmény és az ISMS hatékonyságának értékelése során. Ez lehetővé teszi számára, hogy meghatározza információs igényeit. Ezt megelőzően pedig ehhez a döntéshez a kockázatfelmérés eredménye szolgáltathat bemeneti adatokat.

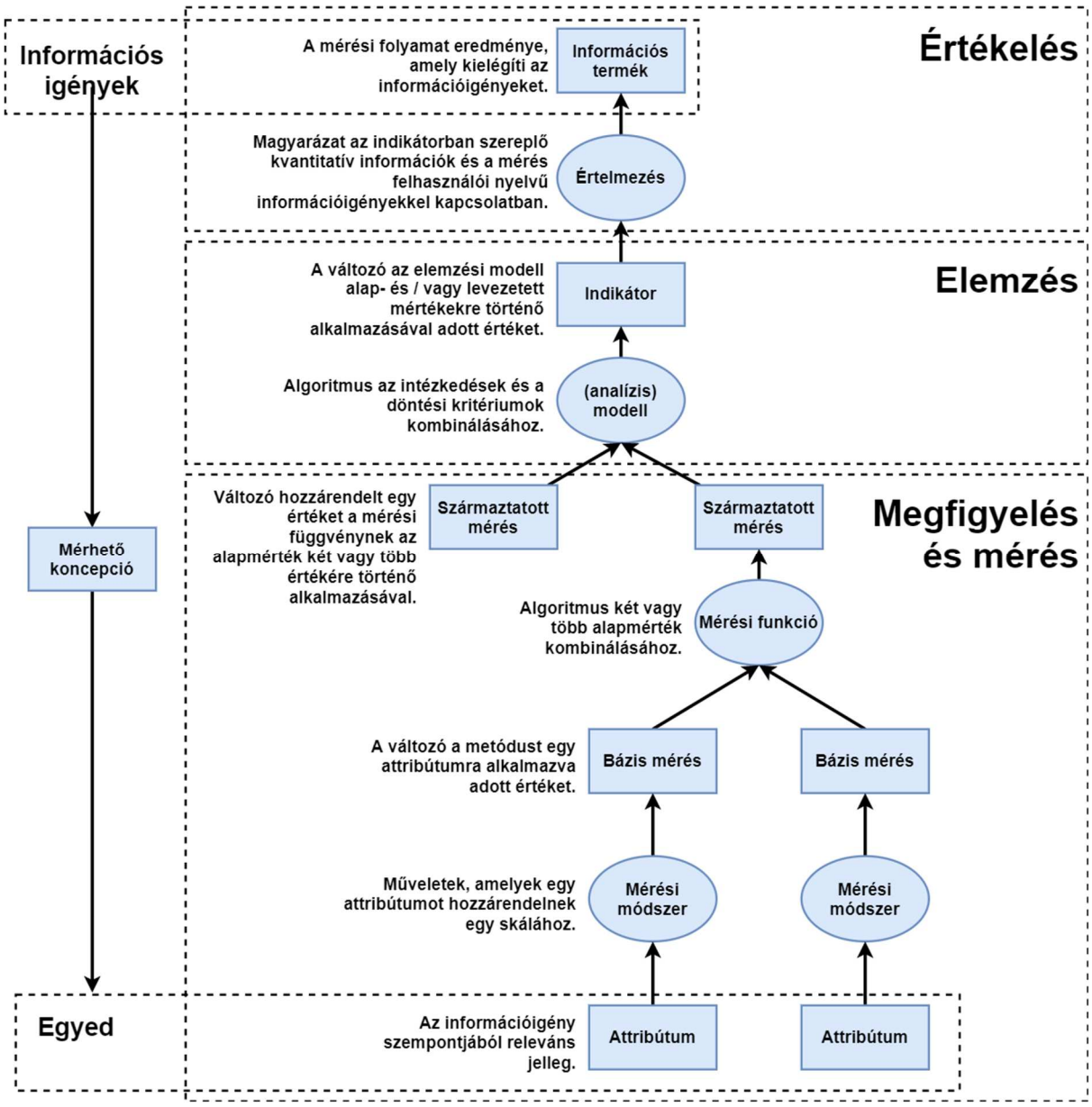
A szervezeteknek el kell dönteniük, hogy milyen intézkedések szükségesek az egyes különálló információigények támogatásához, és milyen adatok szükségesek a szükséges intézkedések levezetéséhez. Ezért a mérésnek mindig meg kell felelnie a szervezet információigényének.

Fel kell tenni a kérdés, hogyan lehetséges ez; Annak meghatározása, hogy melyik munkaszervezet mit mérjen, mire fókuszáljon. Ez egyértelmű, hogy munkaszervezetenként eltérő, egyedi lehet. Természetesen lehet, ROI (return on investment) értékeket, azaz megtérülést számítani, azonban kizárólagos pontként a kockázatértékelés, a kockázat alapú megközelítés lehet az, amely erre választ képes adni. Tehát a kockázatok számítása révén képes lehet a szervezet egy rövidített listával dolgozni, csak az előterjesztett, jóváhagyott méréseket kialakítani, kiértékelni a kockázatok alapján. Ebből egyértelműen következik, hogy a mérések és kiértékelések során, a ciklus végén alkalmazott korrekciós tevékenységek jó esetben befolyásolják a tevékenységet és azon területen mért kockázati értékeket. Tehát akkor a kockázati térkép megváltozásával, a kockázati rangsor (lista) megváltozásával új területre tevődhet át a mérés – kiértékelés – korrektív tevékenység fókusza. Ezt követően pedig a ciklus iterálódik.
Ennyi rövid áttekintés után nézzük meg, hogy milyen további nehézségek, vagy lehetőségek vannak, amelyeket részben mérésekkel is alátámasztott már számos más kutató.



86. ábra: Megfigyelés, mérés, elemzés és értékelés folyamata ISO/IEC 27004:2016 alapján, Forrás: ISO/IEC 27004:2016

Példaként felvillantásként, hogy sokkal komplexebb a mérés megalkotása, … épp ezért kisebb közigazgatási szervezeteknél ennek megvalósítása nem csak költségigényes, de egyenesen kivitelezhetetlen lehet önerőből. Mindezek alátámasztják, hogy nemzeti szinten lenne szükséges kezelni.



87. ábra: Kulcskapcsolatok a mérési információs modellben, ISO/IEC 27004:2016 alapján, Forrás: ISO/IEC 27004:2016 alapján

Az ISO 27001-es szabványcsaládon kívül a NIST Special Publication 800-55 Revision 1 Performance Measurement Guide for Information Security is foglalkozik a kérdéssel. Nemzetközi szinten ezt a két dokumentumot tekinthetjük nem tudományos értelemben alapvetésnek. Megemlítve, hogy az ISO dokumentum csak előfizetéssel érhető el, míg a NIST egy publikus dokumentum. Így a gyakorlatban az ISO szabványcsalás felhasználhatósága csak azon közigazgatási vagy egyéb (jellemzően szervezetekre) korlátozódik, akok ehhez szükséges forrásokkal rendelkeznek.

A mérés igazából valamilyen megfigyelésnek, vagy automatizált adatmintavételnek a kvantifikálásából származik, hiszen az egyén, annak fizikai (SI) mértékegységbeli

tulajdonságaitól eltekintve direktben nem mérhető. Azaz direkt, közvetlen módon nem lehet számszerű mérési eredményeket kinyerni valamely személy információbiztonsági tudatossági szintjéről. Ebből következik, hogy a személyek indirekt mérése és kvantifikálás után ez már a szervezetek, azaz embercsoportok esetében megvalósulhat.

Számos módszer lehet tehát az indirekt mérések lefolytatására és a kvantifikálásra tehát lehetséges (akár automatán) gyűjtött logok, naplóesemények által (viselkedési mintákat elemezve (vagy interjú készítés révén, kérdőíves felmérés révén és ezek kiértékelése révén számszerű eredmények (kvantifikált értékek, számok) állhatnak rendelkezésre. Fontos ismét megemlítenem, hogy ezen értékek a jelenállapot, a változás önmagában korlátozottan, csak kontextusában értelmezhető. Ezen számokat kontextusukban értelmezni kell tudni, mit jelentenek (sok, kevés, elfogadható, határértéken belüli, stb.) További teendőként merül fel, hogy kommunikálni is kell tudni a számokat a vezetőség felé, a cselekvési tervet jóváhagyatni. A fókusz azonban mérésen van, hogyan lehet mérni egy ember, a tudását, különösen azt, hogy ezt a tudást adott helyzetben mennyire akarja vagy mennyire tudja érvényesíteni, mennyire szabálykövető, vagy éppen a tudás hiánya miatt nem tudja követni a szabályzatokat. Ahhoz, hogy a mérés ne csak egy pillanatfelvétel legyen, kontextusba és idősoros elrendezésbe is kell illeszteni. Tehát az egy vagy többféle méréssel felvett és kiértékel adatainkat aztán ha mérünk valamit, akkor meg is kell(ene) tudni ismételni ugyanolyan, vagy másféle módszertannal annak érdekében, hogy a tervezett változást, látni lehessen az elmozdulást a meghatározott időtáv tükrében is. Végül, soha ne felejtsük el, sok esetben a mérés befolyásolhatja a mérendő személyt, vagy az eredményt is, azon vagy a következő mérésre adott eredményeket is, így javasolt kontrollcsoportok alkalmazása, ha tudományos igényességű és nem csupán adott munkaszervezetre érvényes értékeket kívánunk létrehozni.

9. SZÁMÚ MELLÉKLET, 2.2.7. EMBERI TÉVEDÉSEK, LEHETSÉGES HIBÁK

Disszertációm ezen részében, áttekintésjellegűen kitérek a hiba fogalmára és információbiztonsági vonatkozásaira. Mennyire lehet jelentős az emberi hiba az adatok, információ szivárgásában a biztonsági incidensek során? Az adatvédelmi rések, biztonsági kontrollok (részleges) hiánya és az információbiztonság szándékos vagy épp nem szándékozott megsértése számos szervezet számára komoly gondot jelentenek. Az idevonatkozó, logikailag idetartozó leggyengébb láncszem fogalma, valamint a logikailag ide is illeszkedő nem szándékos visszaélések típusai dolgozatomban már említésre kerültek. Ennek lényege, hogy szándékos és

nem szándékos mulasztásra lehet szétválasztani ezen seményeket. A leggyengébb láncszem elmélete pedig arra hívja fel a figyelmet, hogy a lemaradókra, a kockázatos területekre (is) fókuszálni kell, de ahhoz hogy tudjunk ezekről, mérésekre van szükség.

A Magyar értelmező kéziszótár szerint

hiba: A fn 1. Mulasztás v. kifogásolható tett. Hibát követ el; <pongyola haszn:> hibát vét: hibázik, hibát követ el. 2. A gondolkodás, a nyelv v. vmely tudomány szabályait megsértő vétség, tévedés. Szorzási, szórendi hiba. | Tud A helyes értéktől való eltérés. Szórási hiba. 3. Testi, lelki v. erkölcsi fogyatékosság. Szervi hiba. 4. Vmiben tökéletlenség, fogyatékosság. Gyártási hiba. 5. biz Baj, nehézség. Ez nagy hiba; az a hiba, hogy ... 6. biz Hiány, fogyatkozás. Abban nem lesz hiba: az meglesz v. rendben lesz. [szláv]

A Magyar szinonimaszótár (2014) szerint:

hiba

1) [kötelesség nem teljesítéséből eredő] mulasztás; [rendszerint elnézésből v. a valóság félreismeréséből eredő] → tévedés, [(viselkedésbeli) ügyetlenségből származó, kisebb] → baklövés
2) [beszéd, szövegmondás közben elkövetett] → nyelvbotlás
3) [büntetést érdemlő, nagyobb] → vétség (pl. minden vétséget megtorol); [emberi gyöngeségből eredő] gyarlóság (pl. megbocsátható gyarlóság); [mint kifogásolható tulajdonság:] kivetnivaló, régies gáncs (pl. mindenben gáncsot talál)
4) [különösen valaminek a menetében, működésében, felépítésében stb. jelentkező:] rendellenesség, tökéletlenség, sajtónyelvi → hiányosság; → baj (pl. az a baj, hogy…) ‹tágabb értelmű›; [valaminek az előnytelen voltát kiemelve] → árnyoldal (pl. ennek az az árnyoldala, hogy…)
5) hiba nélkül: hibátlanul

Safa et al. (2016) szerint a hibák számos okra vezethetőek vissza: a felhasználó hanyagsága, tudatlansága, tudatosságának hiánya, huncutság, apátia és ellenállás az elsődleges oka az információbiztonsági előírások megsértésének. Ezenkívül vesztegetés, sikkasztás, kémkedés és szabotázs – számos információbiztonsági szabálysértés lehetséges.

Az emberi viselkedés, akár szándékosan, akár figyelmetlenségből fakadóan, nagy kockázati forrást jelenthet az információs eszközökre és a bennük tárolt adatokra nézve. Természetesen tovább bontható szerepkörökre, hogy a végfelhasználók vagy az IT vagy biztonsági rendszerek üzemeltetőire milyen véletlen hibalehetőségek, célzott támadások vagy előírások vonatkoznak. Illetve elemezhető szabálykövetési hajlandóság, motiváció, külső vagy belső szereplők stb.

szerint. Általánosságban elmondható azonban, megállapított tény, hogy a technológia önmagában nem garantálhat biztonságos környezetet az információk és információs eszközök, rendszerek számára; az emberi szempontokat is figyelembe kell venni, valamint a technológiaiakat és eljárásiakat is. Az emberi hiba az ember-gép interfész problémákból, a dolgozókat megterhelő munkakörnyezetből és más szituációs összetevőkből fakad. Disszertációm jelen részében a felhasználók és az információbiztonsági szakemberek által az információbiztonság területén elkövetett hibák feltérképezésére törekszem. Célom, hogy következtetéseimmel tisztázzam az emberi hiba természetét az információbiztonság területén mind az akadémikusok, mind a gyakorlati szakemberek számára, érhetően, a téziseim alátámasztásához szükséges mértékben.

Gyakran nem priorizálják megfelelően a számítógépek és az információs rendszerek biztonságának állandóan fennálló kockázatait, valamint az ezeken a biztonsági rendszereken belüli véletlen és szándékos okok vagy fenyegetések jelentőségét. A szándékos támadások sikerességét gyakrabban okozza a rossz irányítás vagy az operatív gyakorlat, nem pedig az emberi hiba. Ez azonban nem minden esetben igaz, például 2000 őszén a Western Union egy olyan támadás áldozata lett, amelyet inkább emberi hibának, mintsem tervezésinek tulajdonítottak. Egy hacker elektronikus úton engedély nélkül lépett be a Western Union egyik számítógépes szerverére, és mintegy 15 700 ügyfél-hitelkártyaszámot lopott el. Az eset előtt, a rendszert rendszeres karbantartás céljából leállították, és a hitelkártyaadatokat tartalmazó fájl véletlenül védelem nélkül maradt, amikor azt újra működésbe hozták. (Stokes, 2000) Ezenkívül Whitman et al. (2004) megállapította, hogy az információbiztonság igazgatói, menedzserei és felügyelői a műszaki szoftverhibákat és az emberi hibákat magasabbra sorolták, mint a szándékos szoftveres támadásokat. Következtetésem szerint a véletlen okok vizsgálata lehetővé tehetné a szervezetek számára, hogy azonosítsák rendszereikben vagy folyamataikban azokat a gyengeségeket, amelyeket szándékosan ki lehet használni.

Talán a legszélesebb körben ismert és elfogadott emberi hibarendszertan Rasmussen (1982) skillrule-knowledge (SRK) kerete. Ez a keretrendszer feltételezi, hogy a hibákat az egyén teljesítményszintje alapján kategóriákba lehet osztani. A hibákat pszichológiai és szituációs változók egyaránt megkülönböztetik, amelyek együttesen meghatároznak egy „tevékenységi teret", amelyre a három teljesítményszintet leképezik.

A három teljesítményszint a következő: (1) Készségalapú hibák, amelyeket rutinszerű, magasan gyakorlott feladatokkal hajtanak végre, túlnyomórészt automatikus kapacitásban, időnként tudatosan ellenőrizve a haladást. Úgy gondolják, hogy ebben a tevékenységi térben az emberek legtöbbször nagyon jól teljesítenek. (2) A szabályalapú teljesítményszint akkor következik be, ha változtatásra van szükség a készségalapú szinten tapasztalt automatikus viselkedés

módosításához. Ezen a ponton a személy memorizált vagy dokumentált szabályt alkalmazhat, időszakos ellenőrzésekkel a műveletek előrehaladásának és eredményének nyomon követésére. (3) A tudásalapú teljesítmény olyan tevékenységi terület, amely csak ismételt hibázás és teljesítés nélkül valósul meg. Reason (1990); Norman (1983) a hibákat hibaként, tévedésként vagy kihagyásként osztályozták (mistakes or slips and lapses). Ugyanakkor figyelembe kell venni azt is, hogy utólagosan nem mindig osztályozható egyértelműen a hiba. Egyrészt nem lehetséges minden esetben ennek feltárása, másrészt a személyek racionalizálást alkalmaznak, azaz olykor maguknak sem vallják be esetlegesen a pontos gyökérokokat. Vagy egyszerűen észre sem veszik a hibázás tényét. Olyan is lehetséges, hogy a megtévesztés annyira körmönfont, hogy fel sem róható a munkavállalónak az adott szituációban hozott döntés, azaz voltaképpen nem hiba.

Rasmussen (1982) (skillrule-knowledge (SRK) framework) emberiteljesítmény-modelljének felhasználásával a hibákat tovább osztályozom szabályalapú és tudásalapú hibákra. A hibák akkor fordulnak elő, amikor a szándékos cselekvés nem megfelelőnek bizonyult. Ezzel szemben csúszások és tévedések (időbeli elévülések, elfelejtés) akkor fordulnak elő, amikor a cselekvés (vagy a cselekvés hiánya) nem volt szándékos. Hiba lehet például egy nem megfelelő címre küldött e-mail, amely mondjuk incidensbejelentést tartalmaz. Ugyanakkor a bejelentés elmulasztása amiatt, mert a szabály nem ismert, hogy az incidenst jelenteni szükséges, már a cselekvés hiánya, a tudás hiányára vezethető vissza.

Reason (1990) a hibákat szintén a következő kategóriákba sorolta: (i) aktív hiba, amely általában egy komplex rendszerrel való emberi interfész pontján fordul elő; és (ii) látens hiba, amely a rendszer tervezésének hibáit jelenti. A kiváltó okok elemzését általában az esemény mögött rejlő látens hibák feltárására használják. A szerző egy általános hibamodellezési rendszert (GEMS – generic error modeling system) javasolt, amely a hibákat tévedésekbe és hibákba sorolja. A tévedéseket a helyes műveletsorozat helytelen végrehajtásként írja le, a hibák pedig a helytelen műveletsorozat helyes végrehajtására utalnak. A hibák azt a helyzetet képviselik, amikor egy személy rosszul dönt, de a műveletet helyesen hajtja végre. A hibákat „tervezési kudarcnak” nevezi, a tévedést „végrehajtási kudarcnak”. A „hiba” kifejezés értelmezhető szándékos cselekedet eredményeként, amely hibás fogalmi ismereteket, hiányos ismereteket vagy helytelen műveletspecifikációt tartalmaz. Másrészt egy rosszindulatú cselekedet is szándékos, de kár okozására irányul. Így ide sorolható lenne a szabályzatok ismeretének hiánya vagy akár azok pontos, adott munkafolyamatra alkalmazhatósági ismeretének hiánya is.

A tudatosság az információbiztonsági szabályok alkalmazhatóságának, biztosításának egyik legfontosabb eleme, és a felhasználóknak megfelelő információbiztonsági képzésre van szüksége ennek javítása, gyakorlatba átültetése érdekében. A hivatalos prezentációk, e-mailek, játékok,

internetes oldalak, online vagy offline találkozók, poszterek és képernyővédők mind kulcsfontosságú módszernek bizonyultak az egyének tudásának és tudatosságának javítására. (Safa, NS et al., 2015) Ma már a hackerek (is) kreatív, ötletes és újszerű módszereket alkalmaznak céljaik eléréséhez. Bár léteznek a nagy tömegű spam-, átverős kísérletek, ahol abban bíznak, hogy 1% vagy 1 %% biztosan kattint a célszemélyek közül, de sokkal elterjedtebbé váltak a szofisztikált, gondosan megtervezett, akár cégre, személyre szabott támadások mellett az adott biztonsági hibát kihasználó, szintén (apt advanced persistent threat, APT) nagy felkészültséget és jelentős előkészületet igénylő támadások. Ezek akár összetettek is lehetnek, gyakran az előbbiekben vázolt támadási formák mindegyikét ötvözik. Céljaik elérésének érdekében visszaélnek a felhasználók tudatosságának hiányával. Legjellemzőbb kivitelezési forma, hogy első lépésként valamilyen arculat, image, vagy adott személy megszemélyesítése révén egy hiteles információforrás szerepét próbálják átvenni.

Stanton et al. (2005) úgy fogalmaz, hogy számos esetben a tudatlanság az elsődleges oka számos információbiztonság megsértésének. Ez alapvetően most is igaz állítás lehet, azonban az elmúlt évtizedben eltolódtak a támadások a *social enginering* vagy APT támadások irányába. Ilyenek kivédéséhez magasan képzett munkavállalókra van szükség, akik apró jelekre is gyanút fognak, és bejelentik, támogatást kérnek. A tudatlanság, a tudás hiánya vagy a tudás alkalmazási képességének hiánya több tényezőre is visszavezethető: a szabályzatismeret hiánya, a saját munkafolyamatokba ültethetőség meg nem értettsége stb. Stanton és mtsai. (2005) például elemezték a végfelhasználók biztonsági viselkedését, és megállapították, hogy a naiv hibák, például a rossz jelszó-higiénia képezik az alacsony szakértelemmel járó magatartás legnagyobb kategóriáját, amely jelentős hatással van az információbiztonságra. Kutatásaim során bizonyítottam, hogy a jelszóhasználat, általánosítva az azonosítókezelés gyakorlata alkalmas lehet az információbiztonsági szabályok alkalmazási gyakorlatának felmérésére, jellemzésére, kvantifikálására. Törley (2019) így fogalmaz: „A logikai védelem egyik legfontosabb és legtöbb veszélyforrást hordozó része a jelszórendszer.”

A fenyegetések és kockázatok gyakran változnak, emiatt az információbiztonsági képzési programokat rendszeresen frissíteni kell. Voltaképpen a kockázatok változásához szükséges igazítani (mind a szabályzatot, mind pedig) az awareness programot. Az információbiztonsági programoknak a szervezeti kultúra szerves részét kell képeznie az alkalmazottak tudásának és szabályzatalkalmazási képességének naprakészen tartása érdekében. A következetes és releváns intézkedések jelentik az információbiztonsági tudatosság sikerének kulcsát. Az információbiztonsági tudatosság és a támadók által alkalmazott módszerekről való folyamatos tanulás fontos szerepet játszik az információbiztonsági rések kockázatának csökkentésében. Som

(2014) a *gap*ek, (rések, eltérések, melyek a szabályozott vagy elvárt állapot és a gyakorlat között is keletkezhetnek) mint kockázatok felderítését kulcsfontosságú tényezőnek tartja. Az információbiztonsági ismeretek megosztása, az együttműködés és beavatkozás (különböző képzési módszerek) növelik a tudatosság szintjét. (Safa, NS et al., 2016)

A tudatos odafigyelő magatartás azt jelenti, hogy a felhasználók gondolkodnak cselekedeteik információbiztonsági következményeiről, amikor egy számítástechnikai rendszerrel dolgoznak, különösen hogyha az internetet használják. Ez hatékony megközelítés a kreatív támadások leküzdésére és az információbiztonsági rések keletkezési kockázatának csökkentésére. Amikor egy felhasználó gyanús e-mailt kap, amely arra kéri, hogy változtassa meg felhasználónevét vagy jelszavát, adjon meg valamilyen adatot stb., az adathalászattal kapcsolatos tudatossága és tudása beindítja az első riasztást. Elkezd gondolkodni a felhasználónév és jelszó e-mail útján történő megváltoztatásának lehetséges következményein. Vélhetőleg a normál folyamat részeként a levelet bejelenti valamilyen központi rendszerbe, ahol kézi vagy automatizált feldolgozás révén megtörténik a kategorizálása. A szervezeti információbiztonsági irányelvek alapján az alkalmazottaknak nem szabad válaszolniuk az ilyen jellegű e-mailekre, mert a felhasználónév és jelszó bármilyen megváltoztatását hivatalos eljárás során kell végrehajtani. Az egyének tudatossága, tapasztalata és ismeretei, valamint az információbiztonságban való részvétel fontos tényezők, amelyek befolyásolják a tudatos odafigyelő magatartást.

Gawron et al. (2006) az emberi hibát említi más iparágakban a balesetek jelentős okaként. Például az orvosi hiba állítólag a nyolcadik vezető halálok az Egyesült Államokban. A repülési iparban az összes légi fuvarozói baleset háromnegyede az üzemeltető hibáinak tulajdonítható. (Shappell S. et al., 2007) Az online banki tevékenységben a biztonsági fenyegetések állítólag sokkal inkább az emberi tévedésekhez és a rendszerek használhatóságához kapcsolódnak, mint bármely más kérdéshez. (Kjaerland M., 2006) Kraemer és Carayon (2007) felépített egy keretet, amely osztályozza a különböző típusú emberi hibákat, azonosított 216 számítógépes biztonsághoz hozzájáruló szervezeti tényezőt.

Az információbiztonsággal kapcsolatos tanulmányok egyike sem kínált átfogó keretet az emberi tévedések hatásainak enyhítésére, azonban Johnson és Goetz (2007) öt követelményt ajánlott a biztonság szervezetbe építésénél: 1. fókuszváltás a technológiától az emberi viselkedéssel kapcsolatos problémákig, 2. az ügyfelek és üzleti partnerek igényeinek fokozott figyelembevétele a fokozott biztonsággal kapcsolatban, 3. a biztonsági beruházások proaktív megközelítése, 4. a biztonsági mutatók összekapcsolása az üzleti döntéshozatallal és 5. a biztonsági kultúra kiépítése célzott oktatás révén. A GEMS rendszertan azért hasznos, mert egyszerű módot kínál az emberi tévedés legtöbb megnyilvánulásának rögzítésére, és elősegíti a

hibajavítási és -keresési módszerek működését is. Disszertációmban arra törekszem, hogy tömör formában bemutassam az információbiztonság területén elkövetett emberi hibák fajtáit. Ezenkívül leírtam néhány olyan megoldást, amelyet más szakértők korábban már alkalmaztak a fent említett hibák kockázatának csökkentésére. Úgy gondolom, hogy az itt felmerülő kérdések útmutatást nyújthatnak további tudományos kutatásokhoz, illetve menedzserek számára, hogy biztonságosabb környezetet biztosíthassanak az információs eszközöknek. Ezt követően a hibatípusokat vizsgáltam, hiszen az okok feltárása, pontosabb megértése hatékonyan támogathatja a kockázatok csökkentését.

hibatípusok	**indíték**
szándékos	**Előny megszerzése** **Bosszúállás** **Harag** **A munkahely elvesztésétől való félelem** **Öröm és szórakozás** **Megvesztegetés, megtévesztés** **Sikkasztás** **Kémkedés** **Szabotázs**
nem szándékos	**Ellenállás** **Fásultság** **Tudatlanság** **A tudatosság (tudás) hiánya** **Csintalanság** **Gondatlanság**

17. táblázat: Hibatípusok, forrás: Safa és Maple (2016) alapján

A 17. számú táblázatból leolvasható, hogy legalább két jól elkülöníthető hibatípusról van szó, melyeknek további altípusai lehetnek. Az oktatási program során és az incidensek kezelése, kivizsgálása során is ezeket javasolt figyelembe venni, akár kategorizálásnál rögzíteni későbbi statisztikai céllal, amely az oktatási programnál figyelembe vehető.

Kutatásaimnak nem tárgya, nem fő fókusza, de szükségesnek tartom megemlíteni, hogy a tudatosság, kultúra, csopornyomás hármas vonatkozásában szükséges lehet a hiba, a hibázás lehetőségének és kultúrájának kialakítására. Egy klasszikus példát idézve, amikor valaki beszáll a liftbe, és véletlenül rossz emeletet nyom, akkor számos helyen van lehetőség ennek törlésére, azonban, ha más is van a liftben akkor sokan ezt nem teszik meg, mert inkább elrejtik tévedésüket, hibájukat, és annak korrigálására – egyéb okokból – nem törekszenek. Információbiztonsági szempontból fontos kommunikálni, hogy ha történt bármi (esemény), és még akár vétkes is benne az adott felhasználó, sokkal "jobb" az incidenskezelés szempontjából, ha haladéktalanul bejelenti, mintha az eset napokkal később már nem, nehezen vagy akár hatalmas költségek, veszteségek árán korrigálható. Tehát itt kapcsolódik össze a szabályozási környezettel és az ott leírtakkal, hogy bár fontos a szankcióknak transzparensnek lenniük, és azoknak az etikai és egyéb szabályzatokkal szerves egységet alkotni, de meg kell teremteni annak lehetőségét, hogy a véletlen, nem szándékos hiba, félrekattintás esetén elmaradó vagy mérsékelt szankcionálás legyen, valamint ezzel az érintettek tisztában legyenek.

10. SZÁMÚ MELLÉKLET, AZ ISO 27000-ES SOROZAT ELEMEI

ISO/IEC 27000 — Information security management systems — Overview and vocabulary

ISO/IEC 27001 — Information technology - Security Techniques - Information security management systems — Requirements. The 2013 release of the standard specifies an information security management system in the same formalized, structured and succinct manner as other ISO standards specify other kinds of management systems.

ISO/IEC 27002 — Code of practice for information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS

ISO/IEC 27003 — Information security management system implementation guidance

ISO/IEC 27004 — Information security management — Monitoring, measurement, analysis and evaluation

ISO/IEC 27005 — Information security risk management

ISO/IEC 27006 — Requirements for bodies providing audit and certification of information security management systems

ISO/IEC 27007 — Guidelines for information security management systems auditing (focused on auditing the management system)

ISO/IEC TR 27008 — Guidance for auditors on ISMS controls (focused on auditing the information security controls)

ISO/IEC 27009 — Essentially an internal document for the committee developing sector/industry-specific variants or implementation guidelines for the ISO27K standards

ISO/IEC 27010 — Information security management for inter-sector and inter-organizational communications

ISO/IEC 27011 — Information security management guidelines for telecommunications organizations based on ISO/IEC 27002

ISO/IEC 27013 — Guideline on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1 (derived from ITIL)

ISO/IEC 27014 — Information security governance.

ISO/IEC TR 27015 — Information security management guidelines for financial services - Now withdrawn[14]

ISO/IEC TR 27016 — information security economics

ISO/IEC 27017 — Code of practice for information security controls based on ISO/IEC 27002 for cloud services

ISO/IEC 27018 — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors

ISO/IEC TR 27019 — Information security for process control in the energy industry

ISO/IEC 27031 — Guidelines for information and communication technology readiness for business continuity

ISO/IEC 27032 — Guideline for cybersecurity

ISO/IEC 27033-1 — Network security - Part 1: Overview and concepts

ISO/IEC 27033-2 — Network security - Part 2: Guidelines for the design and implementation of network security

ISO/IEC 27033-3 — Network security - Part 3: Reference networking scenarios - Threats, design techniques and control issues

ISO/IEC 27033-4 — Network security - Part 4: Securing communications between networks using security gateways

ISO/IEC 27033-5 — Network security - Part 5: Securing communications across networks using Virtual Private Networks (VPNs)

ISO/IEC 27033-6 — Network security - Part 6: Securing wireless IP network access

ISO/IEC 27034-1 — Application security - Part 1: Guideline for application security

ISO/IEC 27034-2 — Application security - Part 2: Organization normative framework

ISO/IEC 27034-6 — Application security - Part 6: Case studies

ISO/IEC 27035-1 — Information security incident management - Part 1: Principles of incident management

ISO/IEC 27035-2 — Information security incident management - Part 2: Guidelines to plan and prepare for incident response

ISO/IEC 27036-1 — Information security for supplier relationships - Part 1: Overview and concepts

ISO/IEC 27036-2 — Information security for supplier relationships - Part 2: Requirements

ISO/IEC 27036-3 — Information security for supplier relationships - Part 3: Guidelines for information and communication technology supply chain security

ISO/IEC 27036-4 — Information security for supplier relationships - Part 4: Guidelines for security of cloud services

ISO/IEC 27037 — Guidelines for identification, collection, acquisition and preservation of digital evidence

ISO/IEC 27038 — Specification for Digital redaction on Digital Documents

ISO/IEC 27039 — Intrusion prevention

ISO/IEC 27040 — Storage security

ISO/IEC 27041 — Investigation assurance

ISO/IEC 27042 — Analyzing digital evidence

ISO/IEC 27043 — Incident investigation

ISO/IEC 27050-1 — Electronic discovery - Part 1: Overview and concepts

ISO/IEC 27050-2 — Electronic discovery - Part 2: Guidance for governance and management of electronic discovery

ISO 27799 — Information security management in health using ISO/IEC 27002 - guides health industry organizations on how to protect personal health information using ISO/IEC 27002.

11. SZÁMÚ MELLÉKLET, A NEMZETKÖZI SZABVÁNYOK ÉS A KIB AJÁNLÁS ELEMEI

A Trusted Computer System Evaluation Criteria (Biztonságos Számítógépes Rendszerek Értékelési Kritériumai), vagy más néven a „Narancs Könyv” az Egyesült Államok informatikai biztonsági követelményrendszere. Az USA Védelmi Minisztériuma készített 1983-ban. (Szádeczky, 2014)

Az Information Technology Security Evaluation Criteria (Információtechnológia Biztonsági Értékelési Kritériumok) 1.2 változatát az Európai Közösség számára kísérleti célból 1991-ben adták ki. A TCSEC-kel elveit, követelményeit tekintve alapvetően megegyezik. (Muha, Krasznay, 2014)

A TCSEC és az ITSEC csak az informatikai rendszerek (eszközök) logikai védelmével, a biztonság funkcionális és minősítési követelményeivel foglakozik, nem térnek ki az adminisztratív és a fizikai védelem területeire. (Muha, Krasznay, 2014)

A Common Criteria (CC, Közös Követelmények) az Európai Közösség, valamint az amerikai és a kanadai kormányok támogatásával került kidolgozásra. A CC követelmény-rendszerének első három fejezetét kitevő „CC 2.0" dokumentumot ISO/IEC 15408 számon nemzetközi szabványként is kiadták. (Muha, Krasznay, 2014)

A CC létrehozásának célja egy olyan biztonsági követelményrendszer létrehozása volt, amely a – forrásul használt – ITSEC, TCSEC és CTCPEC technikai különbségeit feloldja, és ezzel egy nemzetközileg elfogadott szabvány alapjává válik.

„A Közigazgatási Informatikai Bizottság (KIB) 25. ajánlásaként kiadott Magyar Informatikai Biztonsági Ajánlások (MIBA) című ajánlássorozat fő célja, hogy biztonságos informatikai rendszerek kialakítását és fenntartását segítse elő." (Muha, Krasznay, 2014)

MIBIK

A Magyar Informatikai Biztonság Irányítási Keretrendszere (MIBIK). Az ISO 27000, az ISO/IEC TR 13335 szabványok, továbbá a Security within the North Atlantic Treaty Organisation és az Európai Unió (Európai Unió Tanácsának Biztonsági Szabályzata figyelembe vételével készült.

25/1-1. IBIR

Az Informatikai Biztonsági Irányítási Rendszer a TVEB (PDCA = Plan-Do-Check-Act, Tervezés-Végrehajtás-Ellenőrzés-Beavatkozás) modellen alapul. Ezek a folyamatok lefedik a teljes tevékenységi ciklust, megcélozva az effektív informatikai biztonság irányítását egy folytonos fejlesztési programon keresztül.

25/1-2 IBIK

Az Informatikai Biztonsági Irányítási Követelmények alapját az ISO/IEC 27002:2005, az ISO/IEC TR 13335 nemzetközi szabványok, továbbá a NATO és az Európai Unió releváns szabályozásai képezik.

25/1-3 IBIV

Az Informatikai Biztonság Irányításának Vizsgálata c. vizsgálati módszertan alapját a MeH ITB 8. számú ajánlás, a BS 7799-2:2002 szabvány, és az ehhez kapcsolódó PD 3001 – PD 3005 munkadokumentumok képzik, továbbá az IFIP 199/200 (USA) előírások. Az informatikai biztonság ellenőrzéséhez ad módszertani segítséget.

Az összeállított kérdőívek lefedik az Informatikai Biztonság Irányítási Rendszer (IBIR, ISMS – Information Security Management System) folyamatokat.
Segítségükkel részletesen meghatározhatjuk, hogy az IBIK követelményei mennyiben kerültek megvalósításra.

MIBÉTS

Magyar Informatika Biztonság Értékelési és Tanúsítási Séma. A Common Critéria egyezményhez (2003. október) való csatlakozás után kezdődött meg kidolgozása.

12. SZÁMÚ MELLÉKLET, A SZERZŐ SAJÁT – TÉMÁBA VÁGÓ – PUBLIKÁCIÓINAK IRODALOMJEGYZÉKTŐL ELKÜLÖNÜLŐ SZEREPELTETÉSE

MTMT közlemény és idéző összefoglaló táblázat

Hazai kiadású szakfolyóiratban magyar nyelven megjelent tudományos folyóiratcikk

1.

Som, Zoltán

CCTV-rendszerek interoperabilitás és információbiztonsági megközelítésben

MAGYAR RENDÉSZET 17 : 2 pp. 159-171. , 13 p. (2018)

Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos[3376248] [Admin láttamozott]

2.

Som, Zoltán ; Papp, Gergely Zoltán

Tudásfejlesztés a kiberbűnüldözésben – lehetőségek és kihívások

HADMÉRNÖK 11 : 2 pp. 170-182. , 13 p. (2016)

Teljes dokumentum

Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos[3107341] [Admin láttamozott]

3.

Illéssy, Miklós ; Nemeslaki, András ; Som, Zoltán

Elektronikus információbiztonság - tudatosság a magyar közigazgatásban

INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT 14 : 1 pp. 52-73. , 22 p. (2014)

REAL WoS Teljes dokumentum Matarka

Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos[2586706] [Egyeztetett]

Nyilvános idéző összesen: 1, Független: 1, Függő: 0, Nem jelölt: 0

4.

Som, Zoltán

Kibertudatosság mint várható eredmény, a 2013. L. törvény távlati hatásai: Budapesten 2013. október 25-én a Haza Szolgálatában c. konferencián elhangzott előadás szerkesztett anyaga

TÁRSADALOM ÉS HONVÉDELEM 17 : 3-4 pp. 295-302. , 8 p. (2013)

Egyéb URL Egyéb URL

Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos[2707665] [Egyeztetett]

5.

Som, Zoltán

A közigazgatási informatikai felelősök oktatásának kérdései

HADMÉRNÖK 8 : 4 pp. 223-237. , 15 p. (2013)

REAL Teljes dokumentum Egyéb URL

Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos[2548494] [Egyeztetett]

Magyar nyelvű könyv, szerzőként

1.

Som, Zoltán

Kockázatmenedzsment gyakorlat

Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014) , 93 p.

REAL Teljes dokumentum

Könyv/Szakkönyv (Könyv)/Tudományos[2855310] [Admin láttamozott]

2.

Som, Zoltán

Biztonság támogatása

Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014) , 66 p.

REAL Teljes dokumentum

Könyv/Szakkönyv (Könyv)/Tudományos[2855204] [Admin láttamozott]

Könyvrészlet, idegen nyelvű:

1.

Som, Zoltán

Laws aiding cyber-security in the EU

In: Alexander, Balthasar; Hendrik, Hansen; Balázs, Kőnig; Robert, Müller-Török; Johannes, Pichler (szerk.) Central and Eastern European eGov Days 2014 : eGovernment: Driver or Stumbling Block for European Integration

Wien, Ausztria : Austrian Computer Society, (2014) pp. 115-126. , 12 p.

Könyvrészlet/Szaktanulmány (Könyvrészlet)/Tudományos[2808661] [Admin láttamozott] –

13. MELLÉKLET, KÖSZÖNETNYILVÁNÍTÁS

Ezúton szeretném köszönetemet kifejezni mindazoknak, akik véleményükkel, javaslataikkal, valamint segítő szándékú, konstruktív észrevételeikkel támogatták a disszertációm létrejöttét.

Köszönöm családom türelmét, akik támogattak tudományos erőfeszítéseim alatt.

Köszönöm témavezetőm Dr. Szádeczky Tamás segítségét, kitartó támogatását, értékes tanácsait.

Külön köszönöm Dr. Muha Lajosnak és Dr. Krasznay Csabának szakmai és emberi támogatását, hasznos ötleteket és szakmai meglátássaik megosztását!

Köszönettel tartozom a műhelyvitájám résztvevőinek Dr. Muha Lajosnak, Dr. Péterfalvi Attilának, Dr. Kerezsi Klárának, Dr. Krasznay Csabának, Dr. Fórizs Csabának, Dr. Tóth Andrásnak, Dr. Tarján Gábornak, Dr. Kiss Tibornak, Dr. Novák Mónikának, Dr. Schweickhardt Gothilfnak, Dr. László Gábornak, Dr. Szuhai Ilonának.

Opponenseimnek Dr. Bujdosó Gyöngyinek és Dr. Michelberger Pálnak köszönöm a javaslatokat és az igazán alapos elemzést.

Végül, de nem utolsó sorban köszönetemet szeretném kifejezni a kutatásban részt vetteknek, hogy akik válaszaikkal segítették munkámat.

14. SZÁMÚ MELLÉKLET, A SZERZŐ SAJÁT PUBLIKÁCIÓINAK IRODALOMJEGYZÉKTŐL ELKÜLÖNÜLŐ SZEREPELTETÉSE

MTMT közlemény és idéző összefoglaló táblázat

1. sz. melléklet

Illéssy, Nemeslaki, Som, 2014,

Az IB-tudatosság szintjét mérő kérdőív

Tisztelt Kolléga!

A Közigazgatási és Igazságügyi Minisztérium, a Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Kara és a Vezető-és Továbbképzési Intézet együttműködésében az ÁROP 2.2.17 "Új közszolgálati életpálya" című kiemelt projekt keretében kerül sor a"Nemzeti Közszolgálati Egyetem Közigazgatás-tudományi Karán folyó, vagy beindításra tervezett szakirányú továbbképzési szakok átvilágítása a felhasználói igények megismerése, beazonosítása céljából" című átvilágító kutatásra.

A kutatáson belül az indítás előtt álló elektronikus információbiztonsági menedzser szakirányú továbbképzési szak fejlesztéséhez szükséges ismeretek megszerzésének érdekében végezzük jelen kérdőíves felmérést. A kérdőív célja nem az, hogy személy szerint Önről adatokat gyűjtsünk, hanem hogy felmérjük a közigazgatásban dolgozók átlagos információ-biztonsági tudatosságának szintjét. Ennek megfelelően a kérdésekre nincsenek jó és rossz válaszok, azt szeretnénk kérni Öntől, hogy minden esetben a mindennapi gyakorlatának leginkább megfelelő válaszlehetőséget jelölje be.

A kérdőív 27 kérdésből áll, és kitöltése körülbelül 20 percet vesz igénybe.

Felhívjuk szíves figyelmét, hogy ha megkezdi a kérdőív kitöltését, és azt megszakítva elhagyja az oldalt, a mentett adatok elvesznek, ezért kérjük a kitöltést egyhuzamban végezze el!

A kérdőív kitöltése anonim módon történik. A kitöltött kérdőíveket bizalmasan kezeljük és az adatok összesítése után azokat megsemmisítjük!

Köszönjük, hogy közreműködésével és fáradozásával hozzájárul a kutatás eredményességéhez!

a kutatócsoport tagjai

1) Van-e informatikai-biztonsággal foglalkozó részleg az ön munkahelyén?

1.1 Igen

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

1.2 Nem

2) Tudja-e, kihez kell fordulnia abban az esetben, ha számítógépét feltörték vagy megfertőződött, vírusos?

2.1 Igen

2.2 Nem

3) Talált-e már valaha trójai programot vagy vírust a gépén munka közben?

3.1 Igen

3.2 Nem

4) Ön szerint észrevenné-e, ha számítógépét feltörnék vagy megfertőződne?

4.1 Igen

4.2 Nem

5) Megadta-e már céges jelszavát másnak, akár cégen belül, akár cégen kívül?

5.1 Igen

5.2 Nem

6) Ön szerint inkább igazak vagy inkább hamisak az alábbi állítások?

Állítás Igaz Hamis

6.1 Ha törlök egy dokumentumot a számítógépemről vagy formázom a merevlemezt, minden információ örökre elvész, amit a dokumentum vagy a merevlemez tartalmazott.

6.2 Az én számítógépemen tárolt információk nem értékesek a hekkerek számára, nem én vagyok a célpontjuk

7) Mennyire érzi biztonságosnak a számítógépét a támadásokkal vagy adatlopásokkal szemben?

7.1 Nagyon biztonságos

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

7.2 Biztonságos

7.3 Nem biztonságos

8) Kérjük 1-5-ig terjedő skálán értékelje, mennyire ért egyet az alábbi állításokkal? Jelöljön 1-est, ha teljes mértékben egyetért, 2-est ha egyetért, 3-ast ha nem tudja, 4-est ha nem ért egyet, 5-öst ha teljes mértékben nem ért egyet!

1 2 3 4 5

8.1 A munkahelyem adatainak és infrastruktúrájának a védelme kizárólag az IT-biztonsági részleg feladata

8.2 Nem részesülünk elég képzésben arról, hogyan védhetnénk meg cégünk számítógépeit és adatait.

8.3 Ha a számítógépemen telepítve van a vírusirtó program, akkor az nem fertőződhet meg, hiszen a vírusirtó megállít minden vírust, trójait és férget.

9. Az ön számítógépe automatikusan elvégzi a frissítéseket?

9.1 Igen

9.2 Nem

9.3 Nem tudom

10) Ön mennyire óvatos, amikor egy levél csatolmányát megnyitja?

10.1 Mindig megbizonyosodom afelől, hogy ismerem azt a személyt, akitől a levél jött és hogy vártam már a levelet.

10.2 Ha ismerem a személyt vagy a céget, akitől a levél jött, mindig megnyitom a mellékletet.

10.3 Az e-mail-ekben található mellékletek megnyitása semmilyen veszéllyel nem jár.

11) Tudja, mi az a szélhámos levél és miről ismerheti fel?

11.1 Igen, tudom.

11.2 Nem, nem tudom.

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

12. Az ön gépén a vírusirtó telepítve is van, frissítve is van és be is van kapcsolva.

12.1 Igen.

12.2 Nem.

12.3 Nem is tudom, mit mondjak erre.

12.4 Nem tudom, mi az a vírusirtó.

13) Az ön munkahelyén van arra vonatkozóan előírás, hogy milyen weboldalakat nem látogathat?

13.1 Nem, nincs erre vonatkozóan előírás, azokat a weboldalakat látogathatom munka közben, amelyeket kedvem tartja.

13.2 Vannak bizonyos előírások, amelyek korlátozzák a munkavégzés közben látogatható weboldalakat, de nem tudom pontosan, melyek ezek.

13.3 Igen, vannak erre vonatkozóan előírások, amelyeket ismerek és be is tartok.

14) Az ön munkahelyén van arra vonatkozóan előírás, hogy hogyan használhatja a levelezőrendszerét?

14.1 Nem, nincs erre vonatkozóan előírás, annak küldök olyan e-maileket munka közben, akinek csak akarok.

14.2 Vannak bizonyos előírások, amelyek szabályozzák, hogy kinek és milyen e-maileket küldhetek munka közben, de nem ismerem ezeket.

14.3 Igen, vannak erre vonatkozóan előírások, amelyeket ismerek és be is tartok.

15) Engedélyezett az ön munkahelyén bizonyos felhőszolgáltatások alkalmazása (pl. iCloud, Dropbox, Google Drive) céges adatok tárolására?

15.1 Igen, a felhőszolgáltatások használata engedélyezett

15.2 Nem, a felhőszolgáltatások használata nem engedélyezett

15.3 Nem tudom

16) Használhatja ön saját mobil infokommunikációs eszközeit (pl. okostelefon) céges információk tárolására és átvitelére?

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

16.1 Igen, használhatom

16.2 Nem, nem használhatom

16.3 Nem tudom

16.4 Igen, de csak a cég által nyújtott szolgáltatás igénybe vételével

17) Töltött le és telepített ön már szoftvereket, akár a munkájához kapcsolódóan (pl. PDF-konvertálás vagy képek átméretezése), akár személyes használatra (pl. zenehallgatás) a munkahelyi számítógépén?

17.1 Igen

17.2 Nem

18) Kérte-e már el az ön jelszavát a főnöke vagy valamelyik munkatársa?

18.1 Igen

18.2 Nem

19) A céges informatikai rendszerbe történő bejelentkezéskor ugyanazt a jelszót használja-e, mint a személyes célokra fenntartott fiókjai (pl. twitter,privát e-mail, facebook, iTunes stb.) esetében?

19.1 Igen

19.2 Nem

20) Milyen gyakran fordul elő, hogy céges adatokat kell lemásolnia és hazavinnie annak érdekében, hogy otthon tudjon vele dolgozni.

20.1 Majdnem minden nap

20.2 Legalább hetente egyszer

20.3 Legalább havonta egyszer

20.4 Soha

21) Jelentkezett-e már be a céges informatikai rendszerbe valamilyen nyilvános számítógépről (pl. könyvtárban, hotelben, kávézóban)?

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

21.1 Igen

21.2 Nem

22. Ön általában milyen gyakran változtatja meg jelszavát?

22.1 Naponta

22.2 Hetente

22.3 Havonta

22.4 Félévente

22.5 Évente

22.6 Soha

22.7 A céges rendszer automatikusan figyelmeztet a lejárat előtt és akkor változtatom meg.

23) Kérjük, adja meg születési évszámát!

23.1 ……

24) Az ön neme

24.1 Férfi

24.2 Nő

25) Az ön munkahelye milyen nagyságú településen található: (vagy az a kirendeltsége ahova bejár dolgozni)

25.1 1-5.000 fő

25.2 5.001-10.000 fő

25.3 10.001-20.000 fő

25.4 20.001-50.000 fő

25.5 50.001-100.000 fő

25.6 100.001-250.000 fő

25.7 250.000 fő felett

26) Mi az ön legmagasabb iskolai végzettsége?

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

26.1 Nyolc általános vagy annál kevesebb

26.2 Szakiskola és szakmunkásképző

26.3 Középiskola érettségivel

26.4 Főiskola vagy egyetem

27) Él-e önnel egy háztartásban olyan gyermek, aki még iskolai tanulmányokat folytat?

27.1 Igen

27.2 Nem

MAGYARORSZÁG MEGÚJUL
A projekt az Európai Unió támogatásával, az Európai Szociális Alap társfinanszírozásával valósul meg.

Kontraszt mód aktivál

0%

Üdvözlünk!
A Nemzeti Közszolgálati Egyetem és a Miskolci Egyetem közreműködésével felmérést végzünk abból a célból, hogy képet alkothassunk a jelszóhasználati szokásokról. Kérünk Téged, hogy oszd meg a jelzett kérdéskörrel kapcsolatos tapasztalataidat az alábbiakban olvasható kérdőív kitöltésével. Az adatokat bizalmasan és anonim módon kezeljük. Kér Téged, hogy szakíts időt (kb. 20 percet) a kérdések megválaszolására, és 2015. június 15-ig töltsd ki! Ahol egyszerre több válasz is adható, azt külön feltüntettük. A kérdések egy részénél skála segítségével lehet válaszolni, mellyel a fontosságot lehet kifejezni. Ilyenkor az adott állítás mérlegelése után kérünk, hogy jelöld be a megfelelőnek ítélt értéket.
További kérdés esetén kérlek lépj kapcsolatba velem

Som Zoltán, IT biztonsági szakértő (E-mail: som.zoltan.kdi@office.uni-nke.hu)

1 Demográfiai jellemzők és általános kérdések

1.1	**Nem:**	Kérem, válasszon…
1.2	**Születési év:**	
1.3	**Legmagasabb iskolai végzettség:**	Kérem, válasszon…
1.4	**Mivel foglakozol jelenleg?**	Kérem, válasszon…
1.5	Milyen szférában dolgozol?	Kérem, válasszon…
1.6	**Az üzleti szféra mérete?**	Kérem, válasszon…
1.7	**A közszféra fajtája?**	Kérem, válasszon…
1.8	**A civil szféra típusa?**	Kérem, válasszon…

2 Jelszóhasználat

2.1	Hozzávetőlegesen hány darab különböző jelszót használsz?	
2.2	Van-e olyan jelszavad, ami tartalmaz személynevet?	○ Igen ○ Nem ○ Nem mondom meg
2.3	Van-e olyan jelszavad, ami tartalmaz értelmes szót akár magyarul vagy bármely más nyelven?	○ Igen ○ Nem ○ Nem mondom meg

A jelszavamtól elvárom, hogy .....

2.4	... legyen biztonságos.	Egyáltalán nem fontos	○	○	○	○	○	○	○ Nagyon fontos	○ Nem mondom meg
2.5	... legyen megjegyezhető.	Egyáltalán nem fontos	○	○	○	○	○	○	○ Nagyon fontos	○ Nem mondom meg
2.6	... feleljen meg a jó jelszó elvárásainak.	Egyáltalán nem fontos	○	○	○	○	○	○	○ Nagyon fontos	○ Nem mondom meg
2.7	... meg tudjam védeni az adataimat.	Egyáltalán nem fontos	○	○	○	○	○	○	○ Nagyon fontos	○ Nem mondom meg

2.8	Hány karakter a legrövidebb jelszavad?	
2.9	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	
2.10	Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?	○ Igen ○ Nem ○ Nem mondom meg

2.11	Mennyire jellemző, hogy van valamilyen jelszóházirend, kötelező szabály azokon a helyeken, programokban, amit általában használsz?	Egyáltalán nem jellemző	○	○	○	○	○	○	○ Nagyon jellemző	○ Nem mondom meg

Használsz-e valamilyen jelszóképzési szabályt annak érdekében, hogy ...

2.12	... könnyen megjegyezhető legyen a jelszavadat?	○ Igen ○ Nem ○ Nem mondom meg
2.13	... biztonságos legyen a jelszavad?	○ Igen ○ Nem ○ Nem mondom meg
2.14	Hallottál-e már jelszószéfről (jelszókezelő programokról)?	○ Igen ○ Nem ○ Nem mondom meg/Nem használom
2.15	Ha hallottál a jelszószéfről, akkor használod-e?	○ Igen ○ Nem ○ Nem mondom meg/Nem használom
2.16	Mióta használod a jelszószéfet?	○ Egy hete ○ Egy hónapja ○ Negyed éve ○ Fél évet ○ Egy éve ○ Több mint egy éve ○ Nem mondom meg/Nem használom
2.17	Kérlek írd le pár szóban, hogy mi a jó a jelszószéfben, Neked mi tetszik benne?	
2.18	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	○ Naponta ○ Hetente ○ Havonta ○ Negyed évente ○ Évente ○ Ritkábban, mint évente ○ Soha ○ Nem mondom meg
2.19	Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?	○ Igen ○ Nem ○ Nem mondom meg

2.20 Hány karakter a leghosszabb jelszavad?

2.21 Hány karakter hosszú az, ami nagyon vigyáz az adataidra?

2.22 Van-e olyan információ, amit fontosabbnak tartasz a többinél és jobban meg akarod védeni, ebben az esetben hány karaktert használsz?

2.23 A számodra nagyon fontos adatok esetében hogyan növeled a jelszó jóságát?

Mennyire értesz egyet a következő állításokkal?

2.24	Ha megbízható emberekkel használok közös jelszót, az nem jelent biztonsági kockázatot.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.25	Minden helyre különböző jelszót használok.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.26	Ritkán változtatok jelszót.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.27	Jelszavaimban általában mind a 4 karakter típust (kisbetű(ke)t, nagybetű(ke)t, számo(ka)t és speciális karakter(eke)t) használom.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.28	Saját belátásod szerint, mennyire vagy tisztában a jó jelszóval kapcsolatos elvárásokkal?	Egyáltalán nem	○	○	○	○	○	○	○ Teljes mértékben	○ Nem mondom meg
2.29	Nagyon jók és biztonságosak a jelszavaim.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.30	Az érzékenyebb, fontosabb adatokhoz hosszabb jelszót szoktam használni.	Egyáltalán nem értek egyet	○	○	○	○	○	○	○ Teljes mértékben egyetértek	○ Nem mondom meg
2.31	Figyelembe veszed-e új jelszó megadásánál, ha mutatja az adott alkalmazás a jelszó erősségét?	Nem jellemző	○	○	○	○	○	○	○ Nagyon jellemző	○ Nem mondom meg
2.32	Mennyire jellemző, hogy törekszel az erős jelszóra?	Nem jellemző	○	○	○	○	○	○	○ Nagyon jellemző	○ Nem mondom meg

2.33 Honnan származnak a jelszóval kapcsolatos ismereteid? (Több válasz is lehetséges!)

- ☐ Ismerőstől, baráttól
- ☐ Képzésről, ott tanultam
- ☐ Újság, könyv, televízió, internet
- ☐ Egyéb

2.34 Ha "Egyéb", éspedig....

2.35 Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? ○ Igen ○ Nem ○ Nem mondom meg

2.36 Kérlek fejtsd ki a jelszavakkal, oktatással, biztonsággal kapcsolatos véleményedet pár mondatban.

2.37 Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)

Bármelyik jelszavadra igaz-e, hogy...

2.38	...csak betűket tartalmaz!	○ Igaz	○ Nem	○ Nem mondom meg
2.39	...betűket és számokat is tartalmaz!	○ Igaz	○ Nem	○ Nem mondom meg
2.40	...betűket, számokat és speciális karaktereket is tartalmaz!	○ Igaz	○ Nem	○ Nem mondom meg

2.41 Azon jelszavaknál, amit többen használtok, átlagosan hány ember ismeri azt a jelszót?

2.42	Megadtad-e már valaha másnak, akár csak rövid időre is, ideiglenesen valamelyik jelszavadat?	○ Igen	○ Nem	○ Nem mondom meg
2.43	Ha ideiglenesen adtad meg másnak a jelszavadat bármilyen okból, az ok megszűnése után megváltoztattad-e azt?	○ Igen	○ Nem	○ Nem mondom meg

2.44 Egyéb olyan információ, jelszóval kapcsolatos történet, amit szívesen megosztanál velünk?!

2.45	Véleményed szerint a Te jelszavaid jobbak vagy rosszabbak az ismerőseid által használtaknál?	Sokkal rosszabb	○	○	○	○	○	○	○ Sokkal jobb	○

											Nem mondom meg
2.46	Az érzékenyebb, fontosabb adatokhoz bonyolultabb jelszót szoktam használni!	Nem jellemző	○	○	○	○	○	○	○	Nagyon jellemző	○ Nem mondom meg/Nem használom

2.47 Tudod-e valamelyik ismerősöd bármely jelszavát? ○ Igen ○ Nem ○ Nem mondom meg

2.48 Honnan tudod az ismerősöd jelszavát? ○ Megadta ○ Megszereztem ○ Egyéb ○ Nem mondom meg

2.49 Ha az előző kérdésre egyéb a válasz, akkor kérlek írd le pár szóban az okát!

2.50	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?	Nem jellemző	○	○	○	○	○	○	○	Nagyon jellemző	○ Nem mondom meg
2.51	Mennyire jellemző, hogy a rendszer által minimálisan elvárt jelszóhossznál hosszabbat adsz meg? Tehát ahol mondjuk minimum 8 karakteres jelszót kér a rendszer, ott Te hosszabb jelszót adsz meg	Nem jellemző	○	○	○	○	○	○	○	Nagyon jellemző	○ Nem mondom meg

2.52 Ha meg van adva egy javasolt méret pl. a jelszó legalább 8 karakter legyen, akkor mennyi lesz amit megad?

○ pont annyi amennyi javasolt ○ eggyel több
○ kettővel több ○ hárommal több
○ sokkal több ○ nem mondom meg

3 Informatikai jártasság

3.1 **Hány éve használsz számítógépet?**

3.2 **Hány éve használsz Internetet?**

3.3 **Naponta hány órát töltesz számítógép előtt?**

Milyennek tartod ...

3.4	... a számítógépes alapismereteidet?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.5	... a web-böngészéssel és a hálózati biztonsággal kapcsolatos tudásodat?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.6	... a szövegszerkesztővel kapcsolatos ismereteidet?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.7	... a táblázatkezelővel kapcsolatos tudásodat?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.8	... az adatbázis-kezelővel kapcsolatos ismereteidet?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.9	... a képszerkesztéssel kapcsolatos ismereteidet?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.10	... a prezentáció készítésével kapcsolatos tudásodat?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.11	... a webszerkesztéssel kapcsolatos alapismereteidet?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg
3.12	... az elektronikus hitelességgel, elektronikus aláírással kapcsolatos alapismereited?	Nagyon rossz	○	○	○	○	○	○	○	Nagyon jó	○ Nem mondom meg

Köszönjük, hogy segítettél!
Jelszóval kapcsolatosan ajánlások és érdekességek olvashatóak az alábbi linken!
http://goo.gl/QIYCCx

Elküld

3. sz. m. NKE EIV kérdések

1.	**Mi(k) az információbiztonsági vezető feladata(i)?**
2.	**Mit tehet az információbiztonsági vezető a biztonságért?**
3.	**Kikkel kell együttműködnie az információbiztonsági vezetőnek?**
4.	**Mi az Ön munkaszervezetének a célja, feladata?**
5.	**Az információbiztonsági vezető kiket tud könnyen megnyerni partnernek?**
6.	**Ön szerint mennyi idő alatt lehet változásokat elérni az információbiztonság területén, az Ön munkaszervezetében? (Kérem egy-egy sorban fejtse is ki az önértékelést!)**
	Kérem egy 1-től 7-ig tartó skálán értékelje saját képességeit az alábbi területeken! (Kérem egy-egy sorban fejtse is ki az önértékelést!)
	A) Kommunikáció
	B) Informatika
	C) Projektmenedzsment
	D) Tárgyalástechnika
	E) Információbiztonság
7.	**Saját használatú / tulajdonú számítógépén van-e Önnek rendszergazdai joga?**
8.	**Van-e olyan számítógépe, amit közösen használ a család és Ön is szokott rajta dolgozni?**
9.	**Alkalmazott óvintézkedések?**
10.	**Képzés során érzékelt hiányérzetét adott topic vonatkozásában?**
11.	**Mondjon egy-két olyan folyamatot az Ön munkaszervezetében / vagy általában véve,ahol nem jelenik meg, vagy nem kell, hogy megjelenjen az információbiztonság!**
12.	**Ön hogyan, mennyire vigyáz a pénztárcájára?**
13.	**Ön szerint mi a siker kulcsa?**
14.	**Ön miben méri a sikert?**
15.	**Az Ön vezetője, miben méri a sikert?**
16.	**Az Ön munkaszervezetében megítélése szerint hány darab stratégiai partnere van?**
17.	**A kinevezése óta eltelt időszakról kérem emeljen ki negatív példát! (Amit esetleg kudarcként élt meg!)**
18.	**A kinevezése óta eltelt időszakról kérem emeljen ki pozitív példát! (Amit sikerként élt meg!)**
19.	**Értékelje a szervezeti tudásmenedzsmentet!**
20.	**Az Ön munkaszervezetében hány kulcsember dolgozik?**
21.	**Készült-e erre vonatkozó kockázatelemzés?**

22.	**Jellemezze az eddigiekben bevált kommunikációs stratégiáját (nehéz helyzetekben)!**
23.	**Az Ön munkaszervezetében dolgozók száma? (Akik információbiztonsági szempontból az oktatandók!!) 2 db szám?**
24.	**Tartott-e már a munkaszervezetben információbiztonsági oktatást? Tapasztalatok / mikorra és hogyan tervezi / elképzelések a megvalósításról?**
25.	**Információbiztonsági szabályzat az Ön munkaszervezetében**
	A) Szabályzat B) Gyakorlat
26.	**Ha egy felhasználó eseményt észlel (az Ön munkaszervezetében), hogyan tudja jelenteni?**
27.	**Az információbiztonsági szabályzatnak létezik-e kivonata, kivonatos verziója?**
28.	**Hányszor volt az elmúlt 2 évben szakmai konferencián? Téma / egyéb információ? Megérte-e elmenni / hasznos volt-e az Ön számára?**
29.	**Ön miben látja a problémát?**
30.	**Mi a nehézsége az Ibtv és végrehajtása kapcsán?**
31.	**Mi alapján választották ki Önt erre a pozícióra?**
32.	**Milyen mértékben változtak az információbiztonsággal kapcsolatos ismeretei a képzés kezdete óta?**
	Kérem jelölje meg 1-től 7-ig terjedő skálán, ahol a 7-es legnagyobb mértékben!
33.	**Szokott-e végezni valamilyen önkéntes, karitatív tevékenységet?**
34.	**Mik azok a tényezők amik szükségesek az információbiztonsági program végrehajtásához?**
35.	**Ön mitől hiteles?**
36.	**Ha új belépő van a munkaszervezetben, akkor hol és hogyan jelenik meg az információbiztonsági vetület?**
37.	**Általában az emberek mi alapján hoznak döntéseket?**

4. sz. m. Előadás előtti kérdőív

1.	**Hallott -e már régebben EU Safer Internet programjáról?**
2.	**Ön szerint kitől tanulják a gyermekek az internetezést?**
3.	**Napi hány órát használja az internetet ön?**
4.	**Gyermeke?**
5.	**Több előnye vagy több hátránya van az "internet használatának" ön szerint?**
6.	**Mennyire tartja hasznosnak az internetet a mai világban?**
7.	**Ön szerint mekkora befolyással vannak gyermekére az online csoportok, alkalmazások, játékok?**
8.	**Mennyire használja ezen alkalmazásokat? [Játékok]**
9.	**Ön szerint hány éves kortól lehet használni a facebook-ot?**
10.	**Tudta-e Ön, hogy a Safer Internet ingyenes képzéseket tart?**
11.	**Ön szerint hány oldal terjedelmű az informatikai szabályzat?**
12.	**Ön miért döntött ezen oktatáson való részvétel mellett?**
13.	**Mennyire használja ezen alkalmazásokat? [Közösségi hálózatok]**
14.	**Mennyire használja ezen alkalmazásokat? [Levelezés]**
15.	**Mennyire használja ezen alkalmazásokat? [Chat, videóchat, kapcsolattartás]**
16.	**Mennyire használja ezen alkalmazásokat? [Információ keresés, tájékozódás]**
17.	**Mennyire használja ezen alkalmazásokat? [Tanulás]**
18.	**Mennyire használja ezen alkalmazásokat? [Egyéb (kérem írjon példát!)]**
19.	**Kiket érint a 2013. évi L. törvény?**

5. sz. m. Előadás utáni kérdőív

1.	**Melyik az a weblapcím, vagy kereső kifejezés amit az előadás után fel fog keresni?**
2.	**Mennyire érezte hasznosnak az alábbi témaköröket? [SIP célja]**
3.	**Mennyire érezte hasznosnak az alábbi témaköröket? [Jelszó választás]**
4.	**Mennyire érezte hasznosnak az alábbi témaköröket? [Telefon használat]**
5.	**Mennyire érezte hasznosnak az alábbi témaköröket? [Gyerekekkel való bánásmód]**
6.	**Tudta-e Ön ez előtt, hogy törvény szabályozza az állami szektorban az informatikát, információ védelmet?**
7.	**Milyen témákat látna szívesen a következő előadásokon, milyen kérdések foglalkoztatják Önt, milyen problémára kapna szívesen választ?**
8.	**Mennyire tartja aktuálisnak a rendezvény témáját? Miként ítéli meg a rendezvény témájának aktualitását?**
9.	**Összességében mennyire volt hasznos az Ön számára a rendezvény?**
10.	**Az oktató értékelése különböző szempontok alapján. [Jól kezeli az időt.]**
11.	**Az oktató értékelése különböző szempontok alapján. [Új információt ad.]**
12.	**Az oktató értékelése különböző szempontok alapján. [Érdekes/fenntartja az érdeklődést.]**
13.	**Az oktató értékelése különböző szempontok alapján. [Ajánlaná-e másnak is a munkaszervezetben a tanfolyamot?]**
14.	**Önnek személyes véleménye alapján mi volt ami legjobban tetszett vagy legjobban megragadta a figyelmét?**
15.	**Mennyire valószínű, hogy részt kíván venni a hátralévő két további oktatási modulon? [További modulokon való részvételi szándékom:]**

H1

6. sz. melléklet

One-Sample Kolmogorov-Smirnov Test

Milyen szférában dolgozol?			Hozzávetőlegesen hány darab különböző jelszót használsz?	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Hány karakter a leghosszabb jelszavad?	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	
.	N		484	482	481	462	*
	Normal Parameters[a,b]	Mean	6,88	11,46	14,33	10,42	
		Std. Deviation	11,985	6,820	9,743	13,816	
	Most Extreme Differences	Absolute	0,327	0,228	0,268	0,309	
		Positive	0,323	0,228	0,268	0,309	
		Negative	-0,327	-0,225	-0,235	-0,260	
	Test Statistic		0,327	0,228	0,268	0,309	
	Asymp. Sig. (2-tailed)		,000[c]	,000[c]	,000[c]	,000[c]	
1	N		354	353	352	335	
	Normal Parameters[a,b]	Mean	23,43	12,99	19,22	24,35	
		Std. Deviation	29,876	8,947	14,291	27,424	
	Most Extreme Differences	Absolute	0,283	0,254	0,220	0,250	
		Positive	0,283	0,221	0,220	0,250	
		Negative	-0,228	-0,254	-0,208	-0,205	

	Test Statistic		0,283	0,254	0,220	0,250
	Asymp. Sig. (2-tailed)		,000[c]	,000[c]	,000[c]	,000[c]
2	N		388	385	385	362
	Normal Parameters[a,b]	Mean	9,28	10,12	12,32	11,23
		Std. Deviation	10,834	3,418	6,315	11,341
	Most Extreme Differences	Absolute	0,293	0,192	0,222	0,248
		Positive	0,293	0,192	0,222	0,248
		Negative	-0,238	-0,154	-0,213	-0,209
	Test Statistic		0,293	0,192	0,222	0,248
	Asymp. Sig. (2-tailed)		,000[c]	,000[c]	,000[c]	,000[c]
3	N		5	5	5	4
	Normal Parameters[a,b]	Mean	7,00	11,80	18,20	22,50
		Std. Deviation	5,148	2,588	8,438	38,380
	Most Extreme Differences	Absolute	0,251	0,221	0,234	0,416
		Positive	0,251	0,221	0,234	0,416
		Negative	-0,234	-0,202	-0,184	-0,297
	Test Statistic		0,251	0,221	0,234	0,416
	Asymp. Sig. (2-tailed)		,200[c,d]	,200[c,d]	,200[c,d]	.[c,e]

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. This is a lower bound of the true significance.

e. Significance can not be computed because sum of case weights is less than 5.

*Nagyon sokan nem adták meg a szférát, így nem vehetnek részt a vizsgálatban.

Mann-Whitney Test

Ranks

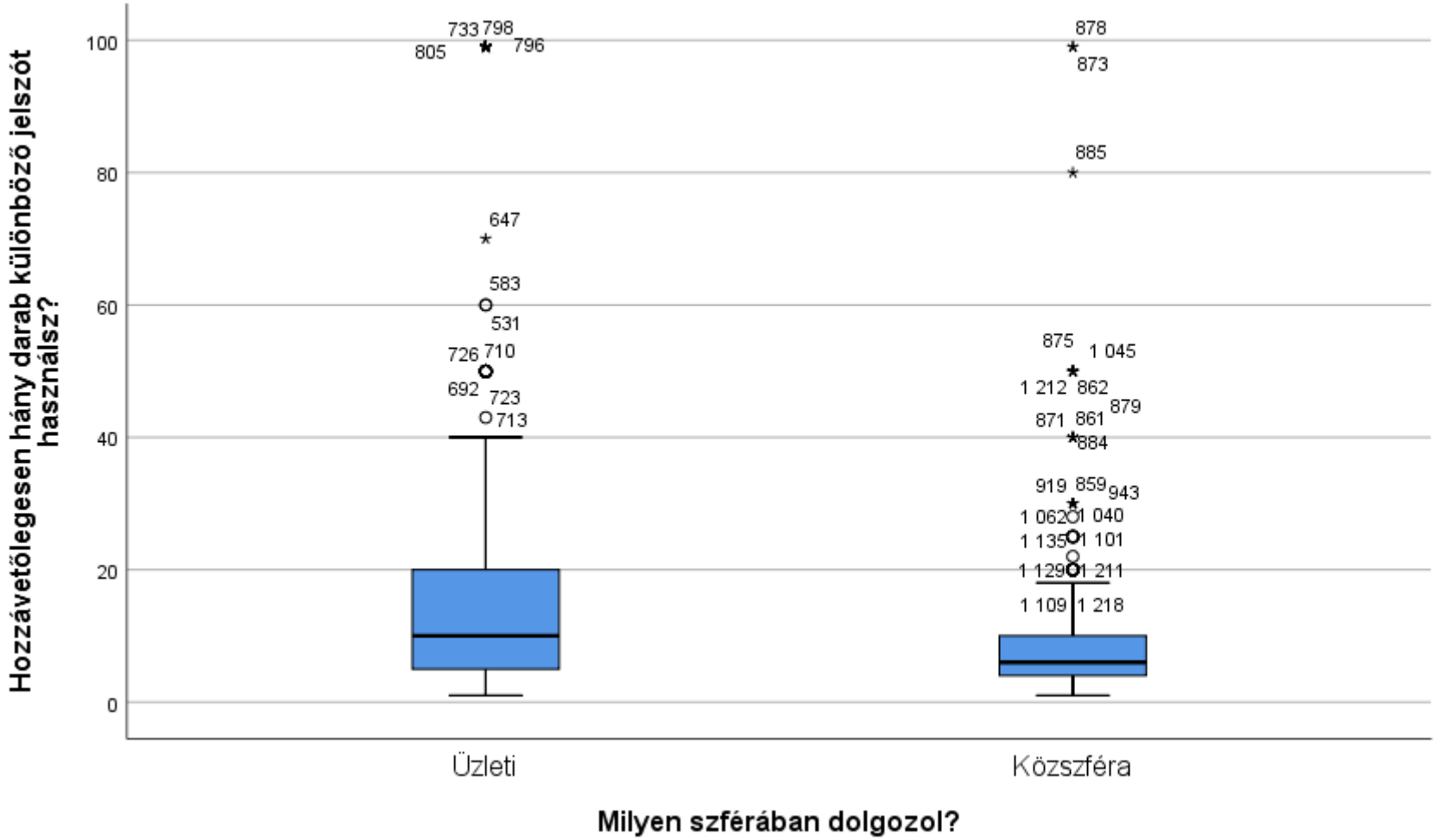
Milyen szférában dolgozol?		N	Mean Rank	Sum of Ranks
Hozzávetőlegesen hány darab különböző jelszót használsz?	Üzleti	354	426,74	151067,50
	Közszféra	388	321,10	124585,50
	Total	742		
Hány karakter hosszú a leggyakrabban, rendszeresen	Üzleti	353	422,19	149031,50
	Közszféra	385	321,19	123659,50
	Total	738		
Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Üzleti	353	381,15	134546,50
	Közszféra	388	361,76	140364,50
	Total	741		
Hány karakter a leghosszabb jelszavad?	Üzleti	352	458,25	161304,50
	Közszféra	385	287,40	110648,50
	Total	737		
Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki	Üzleti	335	407,20	136412,00
	Közszféra	362	295,14	106841,00
	Total	697		
Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba	Üzleti	340	343,62	116831,00
	Közszféra	384	379,22	145619,00
	Total	724		

Test Statistics[a]

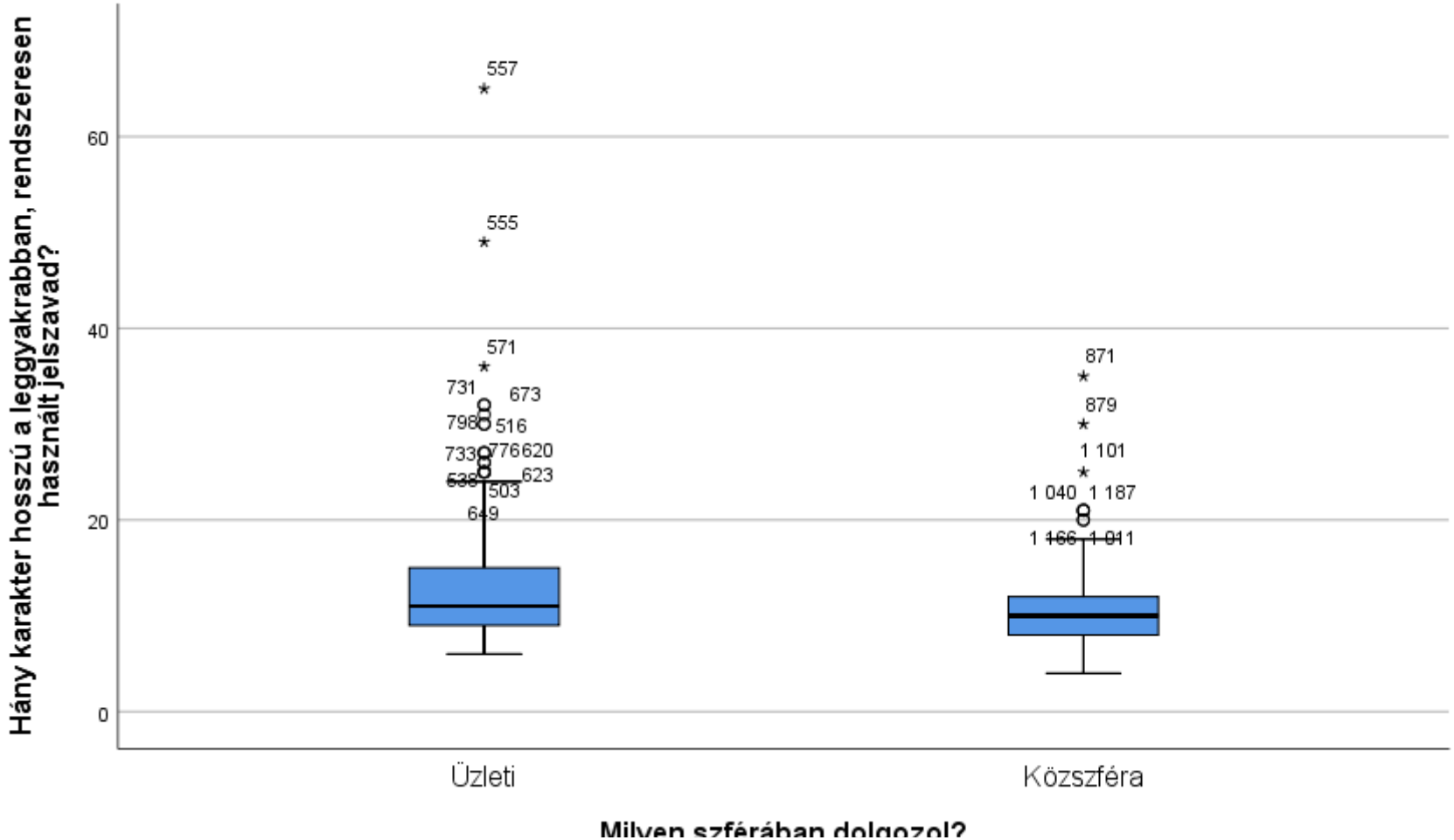
	Hozzávetőlegesen hány darab különböző jelszót használsz?	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Hány karakter a leghosszabb jelszavad?	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?
Mann-Whitney U	49119,500	49354,500	64898,500	36343,500	41138,000	58861,000
Wilcoxon W	124585,500	123659,500	140364,500	110648,500	106841,000	116831,000
Z	-6,739	-6,504	-1,256	-10,929	-7,371	-2,316
Asymp. Sig. (2-tailed)	0,000	0,000	0,209	0,000	0,000	0,021

a. Grouping Variable: Milyen szférában dolgozol?

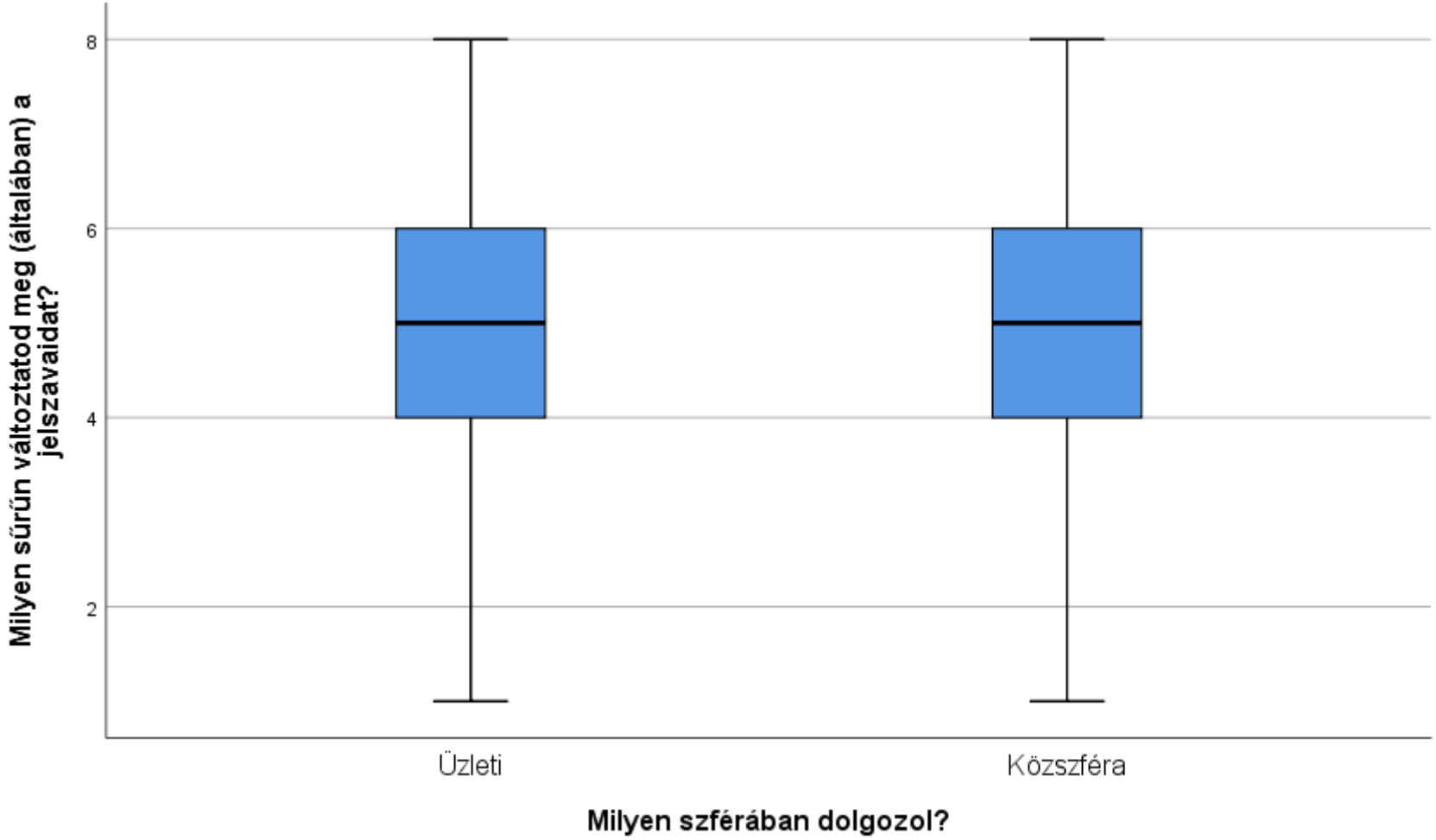
Hozzávetőlegesen hány darab különböző jelszót használsz?



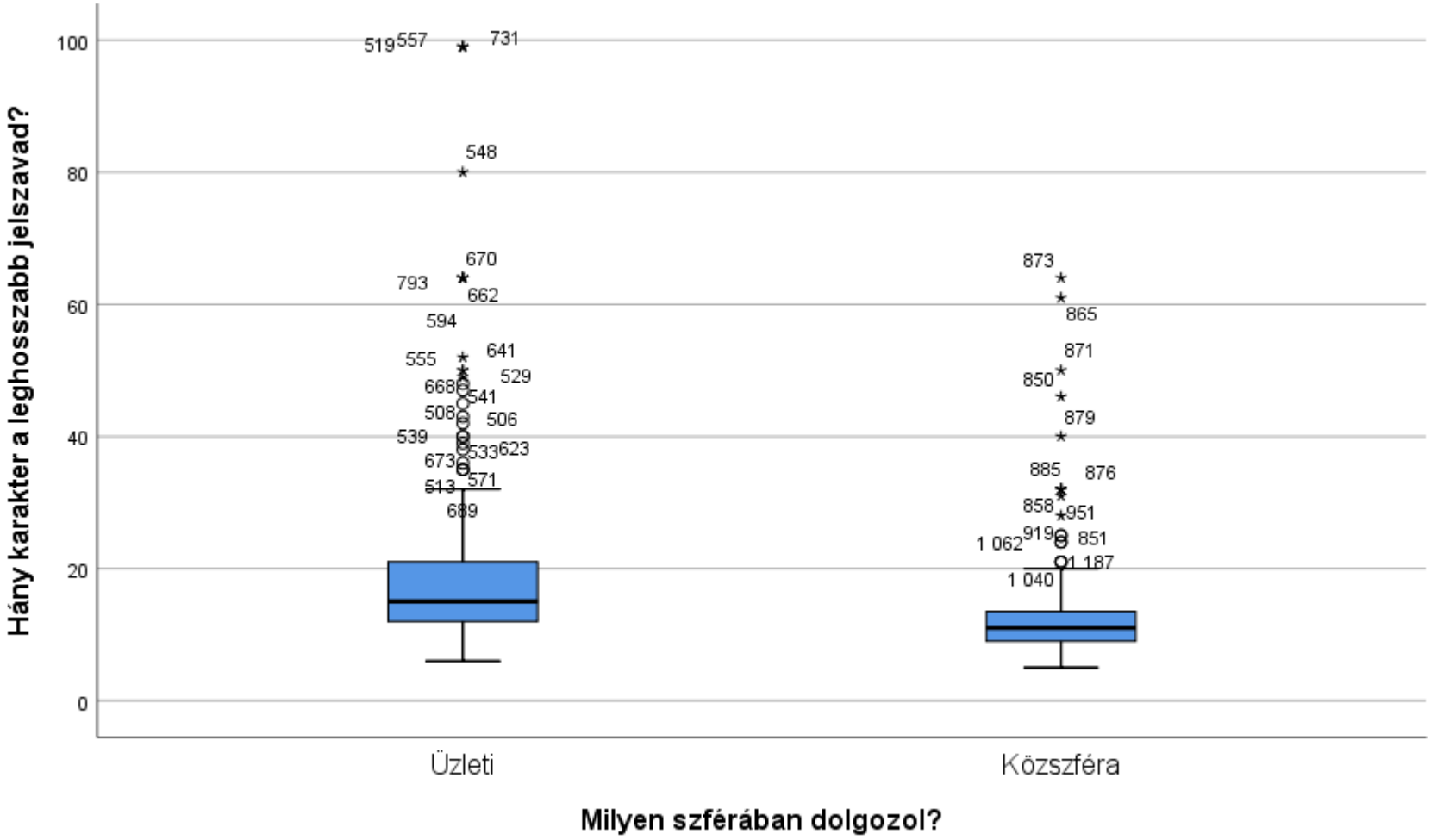
Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?



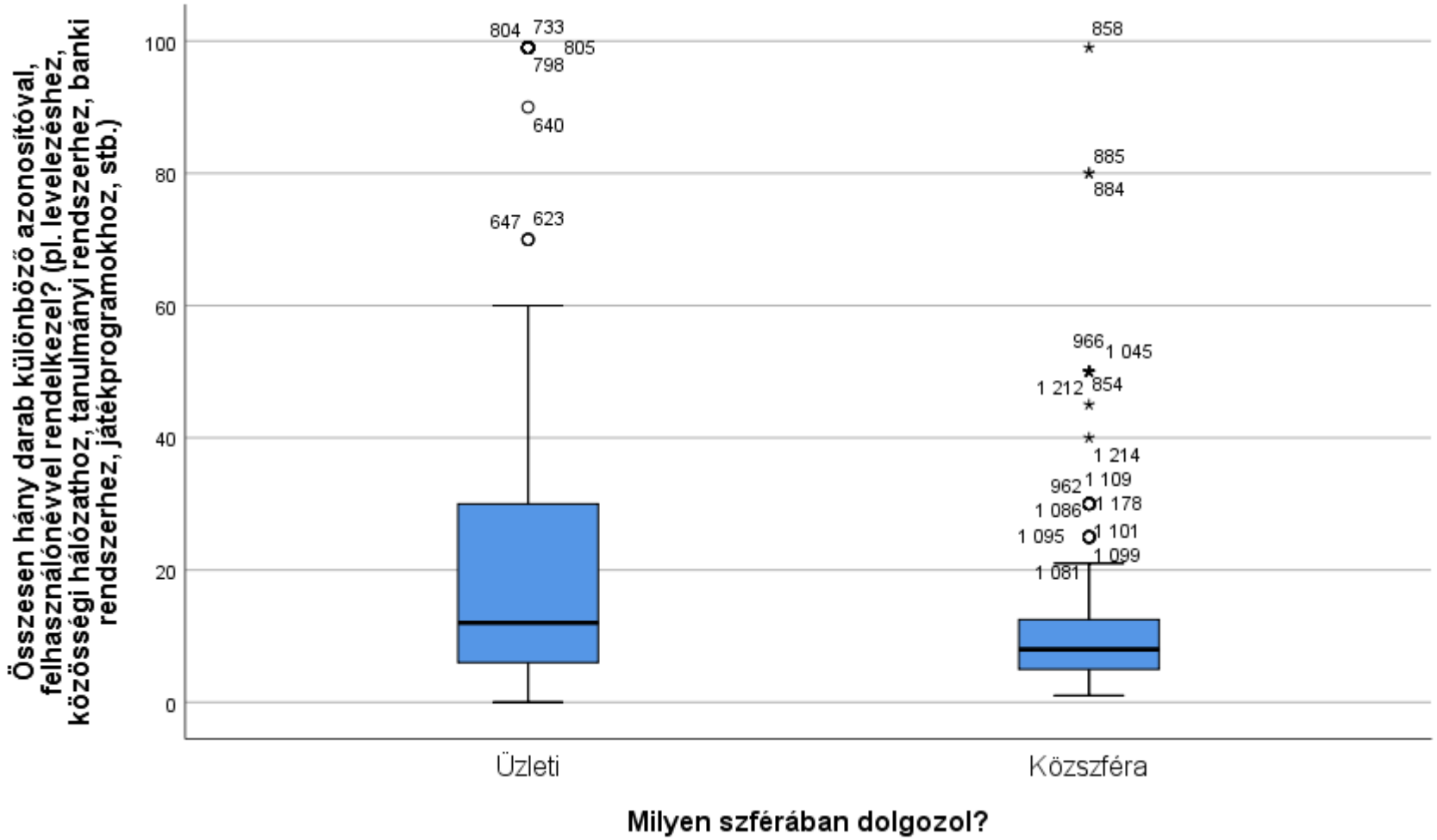
Milyen sűrűn változtatod meg (általában) a jelszavaidat?



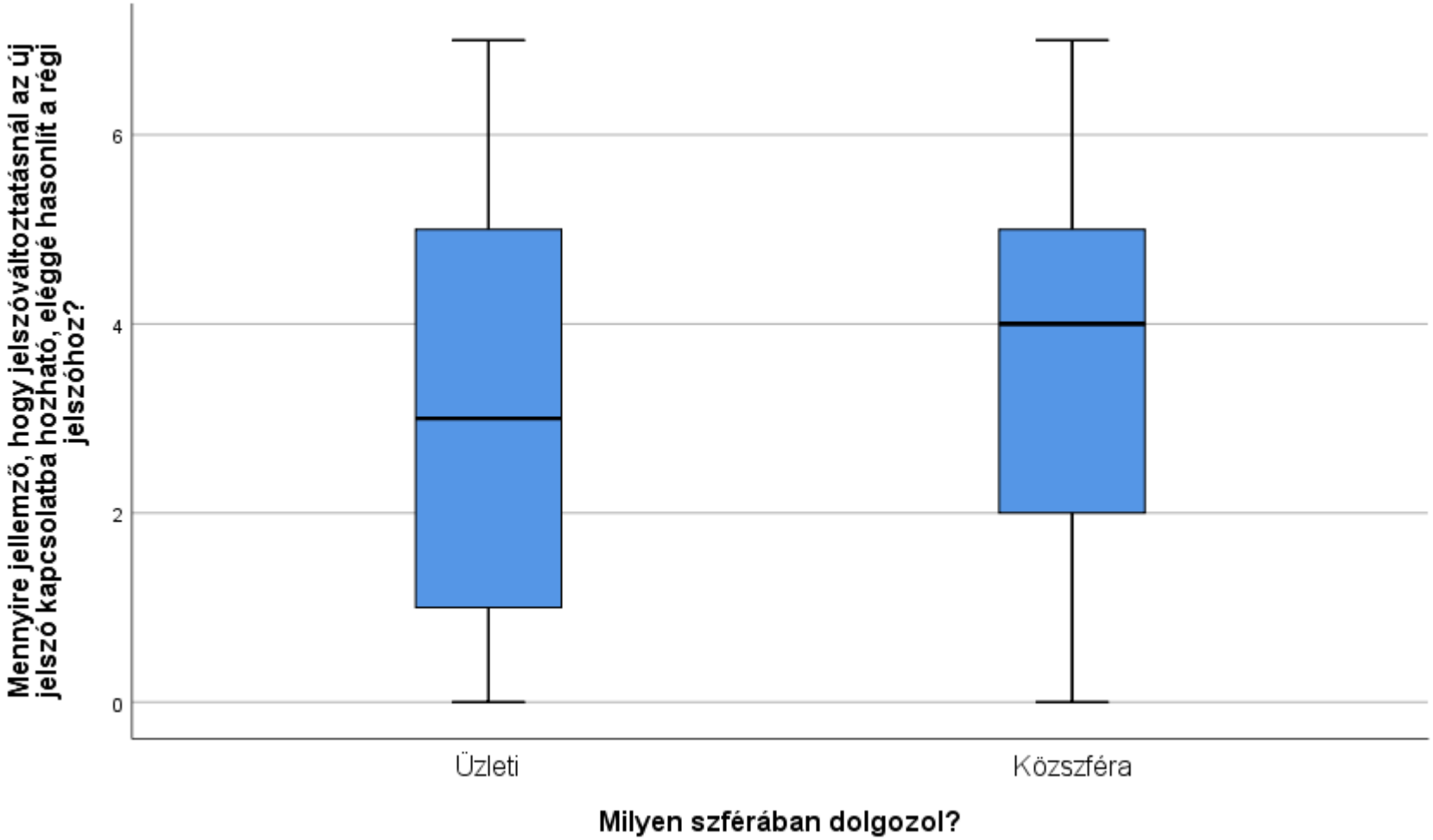
Hány karakter a leghosszabb jelszavad?



Osszesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel?



Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?

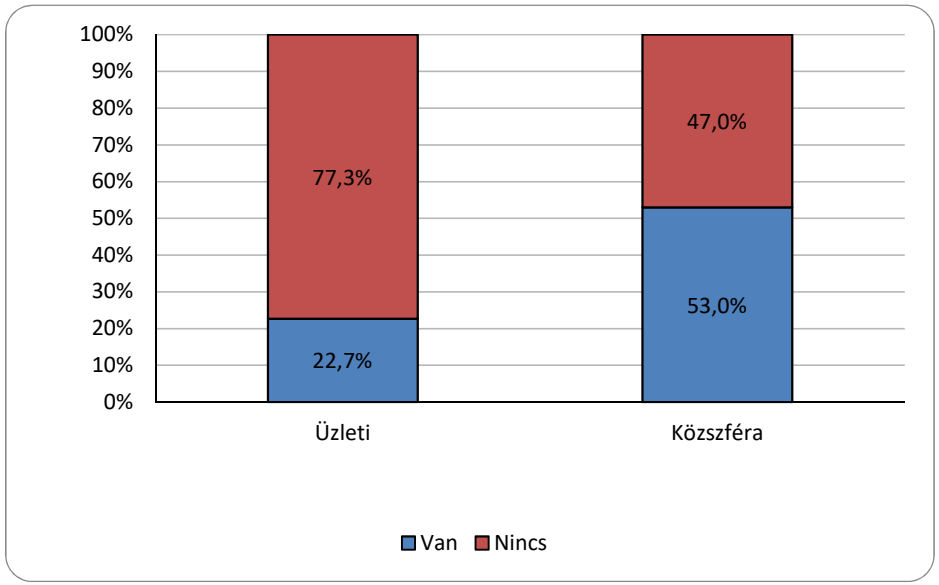


Milyen szférában dolgozol? * Van-e olyan jelszavad, ami tartalmaz személynevet?

Crosstab

			Van-e olyan jelszavad, ami tartalmaz személynevet?		
			Van	Nincs	Total
Milyen szférában dolgozol?	Üzleti	Count	79	269	348
		% within Milyen szférában dolgozol?	22,7%	77,3%	100,0%
		Adjusted Residual	-8,3	8,3	
	Közszféra	Count	195	173	368
		% within Milyen szférában dolgozol?	53,0%	47,0%	100,0%
		Adjusted Residual	8,3	-8,3	
Total		Count	274	442	716
		% within Milyen szférában dolgozol?	38,3%	61,7%	100,0%

Milyen szférában dolgozol? * Van-e olyan jelszavad, ami tartalmaz személynevet?



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	69,456[a]	1	0,000		
Continuity Correction[b]	68,180	1	0,000		
Likelihood Ratio	71,152	1	0,000		
Fisher's Exact Test				0,000	0,000
Linear-by-Linear Association	69,359	1	0,000		
N of Valid Cases	716				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 133,17.

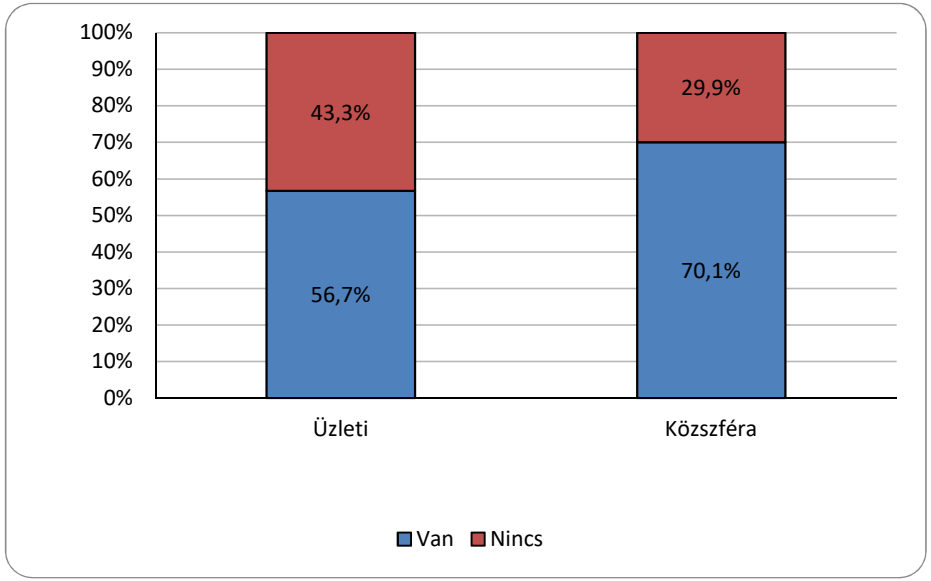
b. Computed only for a 2x2 table

Milyen szférában dolgozol? * Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?

Crosstab

			Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?		
			Van	Nincs	Total
Milyen szférában dolgozol?	Üzleti	Count	194	148	342
		% within Milyen szférában dolgozol?	56,7%	43,3%	100,0%
		Adjusted Residual	-3,7	3,7	
	Közszféra	Count	253	108	361
		% within Milyen szférában dolgozol?	70,1%	29,9%	100,0%
		Adjusted Residual	3,7	-3,7	
Total		Count	447	256	703
		% within Milyen szférában dolgozol?	63,6%	36,4%	100,0%

Milyen szférában dolgozol? * Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	13,534[a]	1	0,000		
Continuity Correction[b]	12,963	1	0,000		
Likelihood Ratio	13,572	1	0,000		
Fisher's Exact Test				0,000	0,000
Linear-by-Linear Association	13,515	1	0,000		
N of Valid Cases	703				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 124,54.

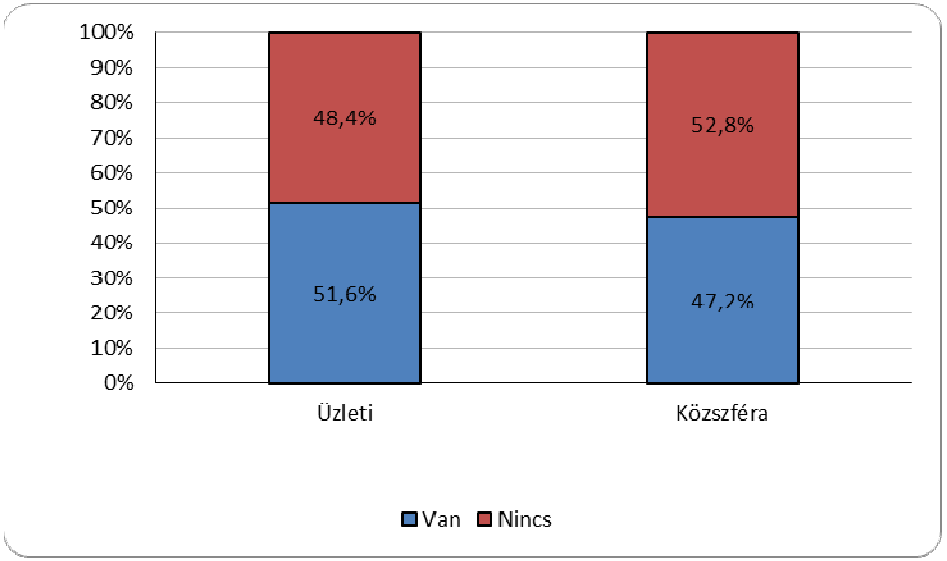
b. Computed only for a 2x2 table

Milyen szférában dolgozol? * Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?

Crosstab

			Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?		
			Van	Nincs	Total
Milyen szférában dolgozol?	Üzleti	Count	181	170	351
		% within Milyen szférában dolgozol?	51,6%	48,4%	100,0%
		Adjusted Residual	1,2	-1,2	
	Közszféra	Count	176	197	373
		% within Milyen szférában dolgozol?	47,2%	52,8%	100,0%
		Adjusted Residual	-1,2	1,2	
Total		Count	357	367	724
		% within Milyen szférában dolgozol?	49,3%	50,7%	100,0%

Milyen szférában dolgozol? * Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?



Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Pearson Chi-Square	1,389[a]	1	0,239		
Continuity Correction[b]	1,219	1	0,269		
Likelihood Ratio	1,390	1	0,238		
Fisher's Exact Test				0,265	0,135
Linear-by-Linear Association	1,387	1	0,239		
N of Valid Cases	724				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 173,08.

b. Computed only for a 2x2 table

Milyen szférában dolgozol? * Van-e olyan jelszavad, ami tartalmaz személynevet? Crosstabulation

% within Milyen szférában dolgozol?

		Van-e olyan jelszavad, ami tartalmaz személynevet?		Total
		Van	Nincs	
Milyen szférában dolgozol?	Üzleti	22,7%	77,3%	100,0%
	Közszféra	53,0%	47,0%	100,0%
Total		38,3%	61,7%	100,0%

Milyen szférában dolgozol? * Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul? Crosstabulation

% within Milyen szférában dolgozol?

		Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?		Total
		Van	Nincs	
Milyen szférában dolgozol?	Üzleti	56,7%	43,3%	100,0%
	Közszféra	70,1%	29,9%	100,0%
Total		63,6%	36,4%	100,0%

Milyen szférában dolgozol? * Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok? Crosstabulation

% within Milyen szférában dolgozol?

		Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?		Total
		Van	Nincs	
Milyen szférában dolgozol?	Üzleti	51,6%	48,4%	100,0%
	Közszféra	47,2%	52,8%	100,0%
Total		49,3%	50,7%	100,0%

H2

7. sz. melléklet.

Mann-Whitney Test

Ranks

Milyen szférában dolgozol?			N	Mean Rank	Sum of Ranks
Üzleti	Hozzávetőlegesen hány darab különböző jelszót használsz?	Kapott oktatást	146	180,06	26288,50
		Nem kapott oktatást	192	161,47	31002,50
		Total	338		
	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Kapott oktatást	148	174,47	25821,00
		Nem kapott oktatást	191	166,54	31809,00
		Total	339		
	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Kapott oktatást	147	165,76	24366,50
		Nem kapott oktatást	192	173,25	33263,50
		Total	339		
	Hány karakter a leghosszabb jelszavad?	Kapott oktatást	147	178,90	26299,00
		Nem kapott oktatást	191	162,26	30992,00
		Total	338		
	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	Kapott oktatást	144	180,62	26009,50
		Nem kapott oktatást	181	148,98	26965,50
		Total	325		
	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?	Kapott oktatást	142	159,16	22601,00
		Nem kapott oktatást	186	168,58	31355,00
		Total	328		

Közszféra	Hozzávetőlegesen hány darab különböző jelszót használsz?	Kapott oktatást	153	213,93	32731,50
		Nem kapott oktatást	229	176,51	40421,50
		Total	382		
	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Kapott oktatást	152	185,72	28229,50
		Nem kapott oktatást	227	192,87	43780,50
		Total	379		
	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Kapott oktatást	152	180,25	27398,50
		Nem kapott oktatást	230	198,93	45754,50
		Total	382		
	Hány karakter a leghosszabb jelszavad?	Kapott oktatást	150	191,31	28697,00
		Nem kapott oktatást	229	189,14	43313,00
		Total	379		
	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	Kapott oktatást	143	195,50	27957,00
		Nem kapott oktatást	213	167,08	35589,00
		Total	356		
	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?	Kapott oktatást	152	188,24	28613,00
		Nem kapott oktatást	226	190,35	43018,00
		Total	378		

Test Statistics[a]

Milyen szférában dolgozol?		Hozzávetőlegesen hány darab különböző jelszót használsz?	Hány karakter hosszú a leggyakrabban, rendszeresen használt jelszavad?	Milyen sűrűn változtatod meg (általában) a jelszavaidat?	Hány karakter a leghosszabb jelszavad?	Összesen hány darab különböző azonosítóval, felhasználónévvel rendelkezel? (pl. levelezéshez, közösségi hálózathoz, tanulmányi rendszerhez, banki rendszerhez, játékprogramokhoz, stb.)	Mennyire jellemző, hogy jelszóváltoztatásnál az új jelszó kapcsolatba hozható, eléggé hasonlít a régi jelszóhoz?
Üzleti	Mann-Whitney U	12474,500	13473,000	13488,500	12656,000	10494,500	12448,000
	Wilcoxon W	31002,500	31809,000	24366,500	30992,000	26965,500	22601,000
	Z	-1,739	-0,744	-0,713	-1,555	-3,028	-0,906
	Asymp. Sig. (2-tailed)	0,082	0,457	0,476	0,120	0,002	0,365
Közszféra	Mann-Whitney U	14086,500	16601,500	15770,500	16978,000	12798,000	16985,000
	Wilcoxon W	40421,500	28229,500	27398,500	43313,000	35589,000	28613,000
	Z	-3,268	-0,632	-1,651	-0,191	-2,567	-0,186
	Asymp. Sig. (2-tailed)	0,001	0,527	0,099	0,849	0,010	0,853

a. Grouping Variable: Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?

Crosstabs

Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? * Van-e olyan jelszavad, ami tartalmaz személynevet?

Crosstab

Milyen szférában dolgozol?				Van-e olyan jelszavad, ami tartalmaz személynevet? Van	Nincs	Total
Üzleti	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	30	113	143
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	21,0%	79,0%	100,0%
			Adjusted Residual	-0,7	0,7	
		Nem kapott oktatást	Count	46	145	191
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	24,1%	75,9%	100,0%
			Adjusted Residual	0,7	-0,7	
	Total		Count	76	258	334
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	22,8%	77,2%	100,0%
Közszféra	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	82	61	143
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	57,3%	42,7%	100,0%
			Adjusted Residual	1,2	-1,2	
		Nem kapott oktatást	Count	111	108	219

		% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	50,7%	49,3%	100,0%
		Adjusted Residual	-1,2	1,2	
	Total	Count	193	169	362
		% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	53,3%	46,7%	100,0%

Chi-Square Tests

Milyen szférában dolgozol?		Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Üzleti	Pearson Chi-Square	,448[c]	1	0,503		
	Continuity Correction[b]	0,289	1	0,591		
	Likelihood Ratio	0,451	1	0,502		
	Fisher's Exact Test				0,513	0,296
	Linear-by-Linear Association	0,447	1	0,504		
	N of Valid Cases	334				
Közszféra	Pearson Chi-Square	1,541[d]	1	0,215		
	Continuity Correction[b]	1,285	1	0,257		
	Likelihood Ratio	1,544	1	0,214		
	Fisher's Exact Test				0,237	0,128
	Linear-by-Linear Association	1,536	1	0,215		
	N of Valid Cases	362				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 49,10.

b. Computed only for a 2x2 table

c. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 32,54.

d. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 66,76.

Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? * Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul?

Crosstab

Milyen szférában dolgozol?				Van-e olyan szó, név, kifejezés, amelyik több jelszavadban is előfordul? Van	Nincs	Total
Üzleti	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	76	67	143
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	53,1%	46,9%	100,0%
			Adjusted Residual	-1,0	1,0	
		Nem kapott oktatást	Count	110	77	187
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	58,8%	41,2%	100,0%
			Adjusted Residual	1,0	-1,0	
	Total		Count	186	144	330

			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	56,4%	43,6%	100,0%
Közszféra	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	106	37	143
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	74,1%	25,9%	100,0%
			Adjusted Residual	1,4	-1,4	
		Nem kapott oktatást	Count	144	70	214
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	67,3%	32,7%	100,0%
			Adjusted Residual	-1,4	1,4	
	Total		Count	250	107	357
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	70,0%	30,0%	100,0%

Chi-Square Tests

Milyen szférában dolgozol?		Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Üzleti	Pearson Chi-Square	1,062[c]	1	0,303		
	Continuity Correction[b]	0,843	1	0,358		
	Likelihood Ratio	1,061	1	0,303		
	Fisher's Exact Test				0,315	0,179
	Linear-by-Linear Association	1,058	1	0,304		
	N of Valid Cases	330				
Közszféra	Pearson Chi-Square	1,909[d]	1	0,167		
	Continuity Correction[b]	1,597	1	0,206		
	Likelihood Ratio	1,929	1	0,165		
	Fisher's Exact Test				0,195	0,103
	Linear-by-Linear Association	1,903	1	0,168		
	N of Valid Cases	357				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 43,00.

b. Computed only for a 2x2 table

c. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 62,40.

d. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 42,86.

Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést? * Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok?

Crosstab

Milyen szférában dolgozol?				Van-e olyan jelszavad, amit rajtad kívül más is tud, esetleg közösen használtok? Van	Nincs	Total
Üzleti	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	73	75	148
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	49,3%	50,7%	100,0%
			Adjusted Residual	-0,8	0,8	
		Nem kapott oktatást	Count	102	88	190
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	53,7%	46,3%	100,0%
			Adjusted Residual	0,8	-0,8	
	Total		Count	175	163	338
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	51,8%	48,2%	100,0%
Közszféra	Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	Kapott oktatást	Count	71	78	149
			% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	47,7%	52,3%	100,0%
			Adjusted Residual	0,2	-0,2	
		Nem kapott oktatást	Count	103	118	221

		% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	46,6%	53,4%	100,0%
		Adjusted Residual	-0,2	0,2	
	Total	Count	174	196	370
		% within Kaptál-e valaha, valahol ezzel kapcsolatos oktatást, képzést?	47,0%	53,0%	100,0%

Chi-Square Tests

Milyen szférában dolgozol?		Value	df	Asymptotic Significance (2-sided)	Exact Sig. (2-sided)	Exact Sig. (1-sided)
Üzleti	Pearson Chi-Square	,633[c]	1	0,426		
	Continuity Correction[b]	0,471	1	0,493		
	Likelihood Ratio	0,633	1	0,426		
	Fisher's Exact Test				0,444	0,246
	Linear-by-Linear Association	0,631	1	0,427		
	N of Valid Cases	338				
Közszféra	Pearson Chi-Square	,039[d]	1	0,843		
	Continuity Correction[b]	0,008	1	0,927		
	Likelihood Ratio	0,039	1	0,843		
	Fisher's Exact Test				0,915	0,463
	Linear-by-Linear Association	0,039	1	0,844		
	N of Valid Cases	370				

a. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 68,35.

b. Computed only for a 2x2 table

c. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 71,37.

d. 0 cells (0,0%) have expected count less than 5. The minimum expected count is 70,07.

8.sz. melléklet

Oneway

Descriptives

Company		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean Lower Bound	95% Confidence Interval for Mean Upper Bound	Minimum	Maximum
A	nincs szabályozás	3	1766,67	76,376	44,096	1576,94	1956,40	1700	1850
	IBSZ publikáció	8	1593,73	270,525	95,645	1367,56	1819,89	1050	1850
	tantermi képzés	13	2834,62	857,172	237,737	2316,63	3352,60	1500	4450
	Total	24	2287,49	882,108	180,059	1915,01	2659,97	1050	4450

Tests of Homogeneity of Variances

Company			Levene Statistic	df1	df2	Sig.
A	bejelentések száma	Based on Mean	5,190	2	21	0,015
		Based on Median	4,409	2	21	0,025
		Based on Median and with adjusted df	4,409	2	13,821	0,033
		Based on trimmed mean	5,150	2	21	0,015

ANOVA

Company		Sum of Squares	df	Mean Square	F	Sig.
A	Between Groups	8555750,260	2	4277875,130	9,617	0,001
	Within Groups	9340874,779	21	444803,561		
	Total	17896625,038	23			

Post Hoc Tests

Multiple Comparisons

Dependent Variable: bejelentések száma

Company		(I) Szakasz	(J) Szakasz	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval Lower Bound	95% Confidence Interval Upper Bound
A	Tukey HSD	nincs szabályozás	IBSZ publikáció	172,942	451,518	0,923	-965,14	1311,02
			tantermi képzés	-1067,949	427,181	0,052	-2144,69	8,79
		IBSZ publikáció	nincs szabályozás	-172,942	451,518	0,923	-1311,02	965,14
			tantermi képzés	-1240,890*	299,693	0,001	-1996,29	-485,49
		tantermi képzés	nincs szabályozás	1067,949	427,181	0,052	-8,79	2144,69
			IBSZ publikáció	1240,890*	299,693	0,001	485,49	1996,29
	Dunnett T3	nincs szabályozás	IBSZ publikáció	172,942	105,320	0,332	-131,70	477,58
			tantermi képzés	-1067,949*	241,792	0,002	-1726,57	-409,33
		IBSZ publikáció	nincs szabályozás	-172,942	105,320	0,332	-477,58	131,70
			tantermi képzés	-1240,890*	256,255	0,001	-1922,31	-559,47
		tantermi képzés	nincs szabályozás	1067,949*	241,792	0,002	409,33	1726,57
			IBSZ publikáció	1240,890*	256,255	0,001	559,47	1922,31

*. The mean difference is significant at the 0.05 level.

One-Sample Kolmogorov-Smirnov Test

Company	Szakasz				bejelentések száma
A	nincs szabályozás	N			3
		Normal Parameters[a,b]	Mean		1766,67
			Std. Deviation		76,376
		Most Extreme Differences	Absolute		0,253
			Positive		0,253
			Negative		-0,196
		Test Statistic			0,253
		Asymp. Sig. (2-tailed)[c]			.[d]
		Monte Carlo Sig. (2-tailed)[e]	Sig.		0,632
			99% Confidence Interval	Lower Bound	0,620
				Upper Bound	0,645
	IBSZ publikáció	N			8
		Normal Parameters[a,b]	Mean		1593,73
			Std. Deviation		270,525
		Most Extreme Differences	Absolute		0,259
			Positive		0,172
			Negative		-0,259
		Test Statistic			0,259
		Asymp. Sig. (2-tailed)[c]			0,121
		Monte Carlo Sig. (2-tailed)[e]	Sig.		0,114
			99% Confidence Interval	Lower Bound	0,106
				Upper Bound	0,122
	tantermi képzés	N			13
		Normal Parameters[a,b]	Mean		2834,62
			Std. Deviation		857,172
		Most Extreme Differences	Absolute		0,135
			Positive		0,135
			Negative		-0,119
		Test Statistic			0,135
		Asymp. Sig. (2-tailed)[c]			,200[f]
		Monte Carlo Sig. (2-tailed)[e]	Sig.		0,741
			99% Confidence Interval	Lower Bound	0,729
				Upper Bound	0,752

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. Significance can not be computed because sum of case weights is less than 5.

e. Lilliefors' method based on 10000 Monte Carlo samples with starting seed 2000000.

f. This is a lower bound of the true significance.

10. sz. melléklet

One-Sample Kolmogorov-Smirnov Test

Company	Szakasz				bejelentések száma
B	IBSZ publikáció	N			9
		Normal Parameters[a,b]	Mean		594,00
			Std. Deviation		91,868
		Most Extreme Differences	Absolute		0,208
			Positive		0,208
			Negative		-0,141
		Test Statistic			0,208
		Asymp. Sig. (2-tailed)[c]			,200[f]
		Monte Carlo Sig. (2-tailed)[e]	Sig.		0,314
			99% Confidence Interval	Lower Bound	0,302
				Upper Bound	0,326
	tantermi képzés	N			10
		Normal Parameters[a,b]	Mean		676,60
			Std. Deviation		216,133
		Most Extreme Differences	Absolute		0,299
			Positive		0,299
			Negative		-0,200
		Test Statistic			0,299
		Asymp. Sig. (2-tailed)[c]			0,011
		Monte Carlo Sig. (2-tailed)[e]	Sig.		0,012
			99% Confidence Interval	Lower Bound	0,009
				Upper Bound	0,014

a. Test distribution is Normal.

b. Calculated from data.

c. Lilliefors Significance Correction.

d. Significance can not be computed because sum of case weights is less than 5.

e. Lilliefors' method based on 10000 Monte Carlo samples with starting seed 2000000.

f. This is a lower bound of the true significance.

11. sz. melléklet

Oneway

Descriptives

Company		N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
B	IBSZ publikáció	9	594,00	91,868	30,623	523,38	664,62	495	759
	e-learning	10	676,60	216,133	68,347	521,99	831,21	495	1254
	Total	19	637,47	170,009	39,003	555,53	719,42	495	1254

ANOVA

bejelentések száma

Company		Sum of Squares	df	Mean Square	F	Sig.
B	Between Groups	32318,337	1	32318,337	1,126	0,303
	Within Groups	487938,400	17	28702,259		
	Total	520256,737	18			

MTMT közlemény és idéző összefoglaló táblázat				
Som Zoltán adatai (2021.10.31)				
Közlemény típusok	**Száma**		**Hivatkozások[1]**	
Tudományos közlemények	Összes	Részletezve	Független	Összes
I. Tudományos folyóiratcikk	5	---	---	---
külföldi kiadású szakfolyóiratban idegen nyelven	---	0	0	0
külföldi kiadású szakfolyóiratban magyar nyelven	---	0	0	0
hazai kiadású szakfolyóiratban idegen nyelven	---	0	0	0
hazai kiadású szakfolyóiratban magyar nyelven	---	5	1	1
II. Könyvek	2	---	---	---
a) Könyv, szerzőként	2	---	---	---
idegen nyelvű	---	0	0	0
magyar nyelvű	---	2	0	0
b) Könyv, szerkesztőként [2]	0	---	---	---
idegen nyelvű	---	0	---	---
magyar nyelvű	---	0	---	---
III. Könyvrészlet	4	---	---	---
idegen nyelvű	---	1	0	0
magyar nyelvű	---	3	0	0
IV. Konferenciaközlemény folyóiratban vagy konferenciakötetben	12	---	---	---
idegen nyelvű	---	5	0	0
magyar nyelvű	---	7	1	2
Közlemények összesen (I.-IV.)	23	---	2	3
Absztrakt[3]	3	---	0	0
Kutatási adat	0		0	0
További tudományos művek[4]	3	---	0	0
Összes tudományos közlemény	29	---	2	3
Hirsch index[5]	1	---	---	---
Oktatási művek	0	---	---	---
Felsőoktatási művek	0	---	---	---
Felsőoktatási tankönyv idegen nyelvű	---	0	0	0
Felsőoktatási tankönyv magyar nyelvű	---	0	0	0
Felsőoktatási tankönyv része idegen nyelven	---	0	0	0
Felsőoktatási tankönyv része magyar nyelven	---	0	0	0
Oktatási anyag	0	---	0	0
Oltalmi formák	0	---	0	0
Alkotás	0	---	0	0
Ismeretterjesztő művek	0	---	---	---
Folyóiratcikk		0	0	0
Könyvek	---	0	0	0
További ismeretterjesztő művek	---	0	0	0
Közérdekű vagy nem besorolt művek[6]	0	---	0	0
További közlemények[7]	0		0	0
Egyéb szerzőség[8]	0	---	0	0
Idézők szerkesztett művekre	---	---	0	0
Idézők disszertációban, egyéb típusban	---	---	0	0

Összes közlemény és összes idézőik	29	---	2	3

Megjegyzések

A táblázat számai hivatkozások is. A számra kattintva a program listázza azokat a műveket, amelyeket a cellában összeszámlált.

--- : Nem kitölthető cella

[1]A hivatkozások a disszertáció és egyéb típusú idézők nélkül számolva. A disszertáció és egyéb típusú idézők összesítve a táblázat végén találhatók.

[2]Szerkesztőként nem részesedik a könyv idézéséből

[3]Csak a tudományos jellegű absztraktok.

[4]Minden további még el nem számolt tudományos mű (kivéve alkotás vagy oltalmi forma), ahol a szerző: szerző, szerkesztő, kritikai vagy forráskiadás készítője szerzőségű.

[5]A disszertációk és egyéb típusú idézők nélkül számolva. A sor értéke az "Összes tudományos közlemény" sor idézettségi adatait veszi alapul.

[6]Minden Közérdekű, Nem besorolt jellegű közlemény, ahol a szerző nem egyéb szerzőségű szerző.

[7]Ide értve minden olyan művet, mely a táblázat más, nevesített soraiban nem került összeszámlálásra.

[8]Minden olyan egyéb szerzőségű mű, ahol a szerző nem: szerző, szerkesztő, kritikai vagy forráskiadás készítője szerzőségű.

2021. okt. 31. 11:44

1.
Som, Zoltán ; Polgár, Zoltán
On overview of information systems and data handling of Hungarian living communities from the perspective of General Data Protection Regulation requirements and information security
In: Nemeslaki, András; Prosser, Alexander; Scola, Dona; Tamás, Szádeczky Central and Eastern European eDem and eGov Days 2019
Wien, Ausztria : Austrian Computer Society, (2019) pp. 459-470. , 12 p.
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[30685050] [Admin láttamozott]

2.
Som, Zoltán ; Jóni, Péter
A Digitális Gyermekvédelmi Stratégia és az állami gondozottak Beszámoló az állami gondozottak körében végzett információbiztonsági (tudatossági) felmérésről
In: Gabos, Erika (szerk.) A média hatása a gyermekekre és fiatalokra IX.
Budapest, Magyarország : Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület (2018) pp. 236-244. , 9 p.
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[30684904] [Admin láttamozott]

3. Som, Zoltán
CCTV-rendszerek interoperabilitás és információbiztonsági megközelítésben
MAGYAR RENDÉSZET 17 : 2 pp. 159-171. , 13 p. (2018)
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[3376248] [Admin láttamozott]

4.
Szádeczky, Tamás ; Polgár, Zoltán ; Som, Zoltán
Communication Security of e-Government Services
In: Juraj, Nemec 25th NISPAcee Annual Conference : Innovation Governance in the Public Sector
Bratislava, Szlovákia : NISPAcee (2017) Paper: 2/11 , 6 p.
Kiadónál ISBN: 9788089013968
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3279286] [Admin láttamozott]

5.
Som, Zoltán ; Szádeczky, Tamás
The legend of information security
In: Hansen, Hendrik; Müller-Török, Robert; András, Nemeslaki; Pichler, Johannes; Prosser, Alexander; Scola, Dona (szerk.) Central and Eastern European eIDem and eIGov Days 2017 : Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?
Wien, Ausztria : Austrian Computer Society (2017) 597 p. pp. 385-398. , 14 p.
REAL
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3229306] [Admin láttamozott]

6.
Som, Zoltán ; Papp, Gergely Zoltán
Információbiztonsági alapok és jelszóhasználati statisztikák: A jelszó, a bizalom és az e-befogadás összefüggései napjainkban
HÍRVILLÁM = SIGNAL BADGE 7 : 1 pp. 47-59. , 13 p. (2016)
Teljes dokumentum
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[3107343] [Admin láttamozott]

7. Som, Zoltán ; Papp, Gergely Zoltán
Tudásfejlesztés a kiberbűnüldözésben – lehetőségek és kihívások
HADMÉRNÖK 11 : 2 pp. 170-182. , 13 p. (2016)
Teljes dokumentum
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[3107341] [Admin láttamozott]

8.
Krasznay, Csaba ; Som, Zoltán
A szülői tudatosság megteremtése a közigazgatási információbiztonsági képzések segítségével
In: Gabos, Erika (szerk.) A média hatása a gyermekekre és fiatalokra VIII
Budapest, Magyarország : Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, (2016) pp. 235-240. , 6 p.
Könyvrészlet/Szaktanulmány (Könyvrészlet)/Tudományos
[3089819] [Admin láttamozott]

9.
Krasznay, Csaba ; Som, Zoltán
Improvement Possibilities Regarding the Training of Electronic Information Security Managers
In: Balthasar, Alexander; Golob, Blaž; Hansen, Hendrik; Müller-Török, Robert; Nemeslaki, András; Pichler, Johannes; Prosser, Alexander (szerk.) Central and Eastern European e|Dem and e|Gov Days 2016 : Multi-Level (e)Governance : is ICT a means to enhance transparency and democracy? : conference proceedings : [... May 12-13, 2016 Budapest]
Vienna, Ausztria : Austrian Computer Society (2016) 607 p. pp. 541-550. , 10 p.
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3089808] [Admin láttamozott]

10.
Som, Zoltán ; Erdősi, Péter Máté ; Papp, Gergely Zoltán ; Pólya, Balázs
Információbiztonsági pillanatkép és helyzetértékelés a magyar közigazgatásban. Különös tekintettel az e-szolgáltatások és e-befogadás, a jelszóhasználati nemzetközi kitekintéssel és az Ibtv. tervezett változásaira, mindezek gazdasági hatására
In: Rajnai, Zoltán; Fregan, Beatrix; Marosné, Kuna Zsuzsanna; Ozsváth, Judit (szerk.) Tanulmánykötet a 6. Báthory-Brassai nemzetközi konferencia előadásaiból. 1-2. kötet
Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2015) 1 372 p. pp. 395-408. , 14 p.
Teljes dokumentum
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3112624] [Admin láttamozott]

11.
Som, Zoltán ; Papp, Gergely
Hungarian Trends in Password Usage, in an International Comparison
In: Alexander, Balthasar; Blaž, Golob; Hendrik, Hansen; Balázs, Kőnig; Robert, Müller-Török; Alexander, Prosser (szerk.) CEE e|Dem and e|Gov Days 2015 : Time for a European Internet?
Wien, Ausztria : Austrian Computer Society, (2015) pp. 299-313. , 15 p.
LUDITA
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3112622] [Admin láttamozott]

12.
Som, Zoltán ; Orbán, Anna
Információbiztonság Magyarországon és Európában - oktatás-fejlesztési lehetőségek az ENISA ajánlások tükrében
In: Haffner, Tamás; Kis Kelemen, Bence (szerk.) Fiatalok Európában Konferencia 2015 absztrakt kötet
Pécs, Magyarország : Sopianae Kulturális Egyesület, (2015) pp. 37-38. , 2 p.
Teljes dokumentum
Könyvrészlet/Absztrakt / Kivonat (Könyvrészlet)/Tudományos
[3109624] [Admin láttamozott]

13.
Som, Zoltán ; Papp, Gergely
The system of conditions for e-acceptance and its development from the point of view of information security
In: Keresztes, Gábor (szerk.) Tavaszi Szél : Absztraktkötet 2015
Budapest, Magyarország, Győr, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ), Publio Kiadó (2015) 485 p. pp. 288-288. , 1 p.
Könyvrészlet/Absztrakt / Kivonat (Könyvrészlet)/Tudományos
[3109623] [Admin láttamozott]

14.
Papp, Gergely ; Som, Zoltán
A e-befogadás feltételrendszere és annak fejlesztése az információbiztonság tükrében
In: Keresztes, Gábor (szerk.) Tavaszi Szél 2015 Konferencia: Konferenciakötet III.
Budapest, Magyarország, Eger, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ), Líceum Kiadó (2015) 664 p. pp. 141-157. , 17 p.
Teljes dokumentum Egyéb URL
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3109621] [Nyilvános]

15.
Som, Zoltán ; Papp, Gergely
Jelszó, bizalom az e-befogadás kérdései napjainkban
In: Kiss, Dávid; Orbók, Ákos (szerk.) A haza szolgálatában 2014 konferencia rezümékötet
Budapest, Magyarország : Nemzeti Közszolgálati Egyetem, (2014) pp. 98-99. , 2 p.
Könyvrészlet/Absztrakt / Kivonat (Könyvrészlet)/Tudományos
[3112623] [Admin láttamozott]

16.
Som, Zoltán
Interoperabilitási kérdések és informatikai biztonsági tükrében a közigazgatásban
In: Rajnai, Zoltán; Fregan, Beatrix; Ozsváth, Judit (szerk.) Az 5. Báthory-Brassai Konferencia tanulmánykötetei
Budapest, Magyarország : Óbudai Egyetem, Biztonságtudományi Doktori iskola (2014) 709 p. pp. 470-480. , 11 p.
REAL Teljes dokumentum
Könyvrészlet/Szaktanulmány (Könyvrészlet)/Tudományos
[3107350] [Admin láttamozott]

17.
Som, Zoltán
Hitelesítési kérdések a magyar (e-) közigazgatásban
In: Csiszár, Imre; Kőmíves, Péter Miklós (szerk.) Tavaszi Szél 2014 Konferencia = Spring Wind 2014: Konferenciakötet II.
Debrecen, Magyarország : Doktoranduszok Országos Szövetsége (DOSZ) (2014) 581 p. pp. 430-443. , 14 p.
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[3107347] [Admin láttamozott]

18.
Som, Zoltán
Kockázatmenedzsment gyakorlat
Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014) , 93 p.
REAL Teljes dokumentum
Könyv/Szakkönyv (Könyv)/Tudományos
[2855310] [Admin láttamozott]

19.
Som, Zoltán
Biztonság támogatása
Budapest, Magyarország : Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014) , 66 p.
REAL Teljes dokumentum
Könyv/Szakkönyv (Könyv)/Tudományos
[2855204] [Admin láttamozott]

20.
Som, Zoltán
Az információbiztonság oktatási kérdései: igények és lehetőségek?
In: Bende, Zsófia (szerk.) A NEMZETI KÖZSZOLGÁLATI EGYETEM KÖZIGAZGATÁS-TUDOMÁNYI KAR KÖZIGAZGATÁS-TUDOMÁNYI DOKTORI ISKOLÁJA 2013/2014-ES TANÉVÉNEK KUTATÓI FÓRUMA : tanulmánykötet
Budapest, Magyarország : Nemzeti Közszolgálati Egyetem, Közigazgatástudományi Kar, (2014) pp. 69-77. , 9 p.
Könyvrészlet/Konferenciaközlemény (Könyvrészlet)/Tudományos
[2850834] [Admin láttamozott]

21.
Som, Zoltán
Laws aiding cyber-security in the EU
In: Alexander, Balthasar; Hendrik, Hansen; Balázs, Kőnig; Robert, Müller-Török; Johannes, Pichler (szerk.) Central and Eastern European eGov Days 2014 : eGovernment: Driver or Stumbling Block for European Integration
Wien, Ausztria : Austrian Computer Society, (2014) pp. 115-126. , 12 p.
Könyvrészlet/Szaktanulmány (Könyvrészlet)/Tudományos
[2808661] [Admin láttamozott]

22.
Som, Zoltán
Cyber security legislation in the EU pp. 1-1. , 1 p. (2014)
poszter, http://www.nispa.org/files/conferences/2014/posters/Zoltan-SOM_Cyber-security-legislation-in-EU-Poster-NISPAcee-2014-Budapest.pdf, Megjelenés: Magyarország,
Teljes dokumentum
Egyéb/Kutatási jelentés (közzétett) (Egyéb)/Tudományos
[2808657] [Admin láttamozott]

23.
Som, Zoltán ; Sasvári, Péter
Az információbiztonság-tudatosság vizsgálata a magyar üzleti- és közszférában
In: ITBN - Informatikai Biztonság Napja - National Day of IT Security
Budapest, Magyarország (2014) pp. 1-23. , 23 p.
Egyéb URL
Egyéb konferenciaközlemény/Konferenciaközlemény (Egyéb konferenciaközlemény)/Tudományos
[2744435] [Egyeztetett]

Nyilvános idéző összesen: 2, Független: 1, Függő: 1, Nem jelölt: 0

24.
Illéssy, Miklós ; Nemeslaki, András ; Som, Zoltán
Elektronikus információbiztonság - tudatosság a magyar közigazgatásban
INFORMÁCIÓS TÁRSADALOM: TÁRSADALOMTUDOMÁNYI FOLYÓIRAT 14 : 1 pp. 52-73. , 22 p. (2014)
REAL WoS Teljes dokumentum Matarka
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[2586706] [Egyeztetett]

Nyilvános idéző összesen: 1, Független: 1, Függő: 0, Nem jelölt: 0

25.
Som, Zoltán
Tudatosság oktatás az infobiztonsági törvény alapján, közigazgatási tapasztalatok
In: Keleti, Arthur (szerk.) ITBN - Informatikai Biztonság Napja - National Day of IT Security
(2013) pp. 1-7. , 7 p.
Egyéb konferenciaközlemény/Konferenciaközlemény (Egyéb konferenciaközlemény)/Tudományos
[2808674] [Admin láttamozott]

26.
Som, Zoltán
A NAT és a biztonságos internetoktatás kapcsolata, kibertudatosság különböző színtereken
In: Gabos, Erika (szerk.) A média hatása a gyermekekre és fiatalokra. VII.
Budapest, Magyarország : Nemzetközi Gyermekmentő Szolgálat Magyar Egyesület, (2013) Paper: kibertudatosság
Könyvrészlet/Szaktanulmány (Könyvrészlet)/Tudományos
[2808655] [Admin láttamozott]

27.
Som, Zoltán
Kibertudatosság mint várható eredmény, a 2013. L. törvény távlati hatásai: Budapesten 2013. október 25-én a Haza Szolgálatában c. konferencián elhangzott előadás szerkesztett anyaga
TÁRSADALOM ÉS HONVÉDELEM 17 : 3-4 pp. 295-302. , 8 p. (2013)
Egyéb URL Egyéb URL
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[2707665] [Egyeztetett]

28. Som, Zoltán
A közigazgatási informatikai felelősök oktatásának kérdései
HADMÉRNÖK 8 : 4 pp. 223-237. , 15 p. (2013)
REAL Teljes dokumentum Egyéb URL
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[2548494] [Egyeztetett]

29.
Som, Zoltán
Az internet veszélyei és ajánlás ennek kezelésére, elsősorban a tizenéves általános iskolások vonatkozásában.
MÓDSZERTANI KÖZLEMÉNYEK: TANÍTÓK ÉS TANÁROK SZÁMÁRA 2012- 53 : 2 pp. 21-32. , 12 p. (2013)
REAL SZTE Egyetemi kiadványok Teljes dokumentum Matarka
Folyóiratcikk/Szakcikk (Folyóiratcikk)/Tudományos
[2347723] [Egyeztetett]